Avaya C460 SMON User Guide

August 2003

Avaya C460 SMON 5.2 User Guide

Copyright 2003 Avaya Inc. All Rights Reserved

The products, specifications, and other technical information regarding the products contained in this document are subject to change without notice. All information in this document is believed to be accurate and reliable, but is presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this document. Avaya disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

Avaya™, Cajun™, P550™, LANstack™, CajunView™, and SMON™ are trademarks of Avaya Inc.

© 2003 Avaya Inc. All rights reserved. All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Release 3.003

Table of Contents

Preface

Welcome to Avaya C460 SMON. This chapter provides an introduction to the structure and assumptions of the guide. It includes the following sections:

- **The Purpose of This Guide** - A description of the intended purpose of this guide.
- **Who Should Use This Guide** - A description of the intended audience of this guide.
- **Organization of This Guide** - A brief description of the subjects covered in each chapter of this guide.

The Purpose of This Guide

This guide contains the information needed to operate the Avaya C460 SMON switch monitoring application efficiently and effectively.

The following table provides information about where to find documentation about Enterprise SMON and Device SMON for other devices.

Table 1. SMON Documentation

Application	Document
Enterprise SMON	*Avaya MultiService SMON User Guide*
Device SMON for Avaya M770 and M-MLS Devices	*Avaya M770 and M-MLS SMON User Guide*
Device SMON for Avaya P120 Devices	*Avaya P120 SMON User Guide*
Device SMON for Avaya P130 Devices	*Avaya P130 SMON User Guide*
Device SMON for Avaya P330 Devices	*Avaya P330 SMON User Guide*
Device SMON for Avaya P580/P882 Devices	*Avaya P580/P882 SMON User Guide*

Who Should Use This Guide

This guide is intended for use by network managers familiar with network management and its fundamental concepts. It is assumed that the user has the basic responsibility for monitoring Avaya Technologies' intelligent switching devices and the network traffic.

Organization of This Guide

This guide is structured to reflect the following conceptual divisions:

- **Preface** - This chapter describes the guide's purpose, intended audience, and organization.
- **SMON Overview** - This chapter provides an overview of the RMON standard and Avaya Inc.'s SMON concepts and an introduction to the SMON tools.
- **Using the Device SMON** - This chapter describes how to launch Avaya C460 SMON and the Device SMON tools. It also describes the Device SMON user interface.
- **Using Switch Statistics** - This chapter describes the Switch Statistics tool in detail, including sample screens and filtering options.
- **Using Port Statistics** - This chapter describes the Port Statistics tool in detail, including sample screens and filtering options.
- **Using Extended Port Statistics** - This chapter describes the Extended Port Statistics tool in detail, including sample screens and filtering options.
- **Using VLAN Statistics** - This chapter describes the VLAN Statistics tool in detail, including sample screens and filtering options.
- **Using Alarms and Events** - This chapter describes the Alarms Table and Alarm Wizard in detail.
- **Using AnyLayer SMON** - This chapter describes the AnyLayer tools in detail.
- **Using Protocol Distribution and DSCP Statistics** - This chapter describes the Protocol Distribution and DSCP tools in detail.

The following Appendices are included at the end of this guide:

- **Using Avaya C460 SMON Dialog Boxes** - Dialog boxes that appear in SMON tools.
- **Setting Up the SMON License** - How to set up the SMON license so that SMON will work with Avaya C460 Devices.

1 SMON Overview

This chapter describes SMON, Avaya Inc.'s switched network monitoring system. This chapter includes the following sections:

- **What is RMON** - A brief description of the RMON standard.
- **What is SMON** - A general description of SMON switch monitoring technology.
- **Overview of SMON** - An introduction to SMON.
- **Device SMON Tools** - The Device SMON tools and how they function.
- **AnyLayer SMON Tools** - The anylayer SMON tool and how they function.

What is RMON

RMON is the internationally recognized and approved standard for detailed analysis of shared Ethernet and Token Ring media. It ensures consistency in the monitoring and display of statistics between different vendors.

RMON's advanced remote networking capabilities provide the tools needed to monitor and analyze the behavior of segments on a network. In conjunction with an RMON agent, RMON gathers details and logical information about network status, performance, and users running applications on the network.

An RMON agent is a probe that collects information about segments, hosts, and traffic, and sends it to a management station.

The network administrator uses software tools to view the information collected by the RMON agent on the management station.

RMON has two levels:

- RMON I analyzes the MAC layer (Layer 2 in the OSI seven-layer model).
- RMON II analyzes the upper layers (Layers 3 and above).

RMON is an industry standard that Avaya Inc. and other companies have adopted in their network management applications. SMON takes the RMON standard and extends it to the switching environment.

What is SMON

SMON is an extension of the RMON standard. SMON adds to the monitoring capabilities of RMON in the following ways:

- It provides additional tools and features for monitoring in the switch environment.
- It provides a global view of traffic flow in a network with multiple switches.

Device SMON extends RMON I for the MAC layer, and AnyLayer SMON extends RMON II for the network layer and above. SMON monitoring collects and displays data in real-time.

Using SMON monitoring, you can get:

- A global view of traffic for all switches on the network.
- An overall view of traffic passing through a specific switch.
- Detailed data about the hosts transmitting packets through a switch.
- An analysis of traffic passing through each port connected to a switch.
- A view of traffic between various hosts connected to a switch.

Overview of SMON

SMON is an RMON-compliant network management suite that implements the SMON extensions to RMON. SMON works with the other components of Avaya MultiService Network Manager to provide a full spectrum of in-depth monitoring of switch traffic and network performance.

SMON consists of a software console application on a workstation and remote monitoring probes in network devices that support SMON.

The SMON console communicates constantly with the SMON devices on your network. The console uses the SNMP protocol to gather information from the devices. SMON provides a suite of powerful graphic display tools to view this information.

SMON gives you detailed analysis of the traffic flow on your switched network, from a global view down to a specific host, and from total MAC layer traffic down to a specific application protocol - all in real-time.

In addition, SMON allows you to set alarms based on traffic thresholds. When an alarm is triggered, a trap can be sent to the device's manager, and the event that triggered the alarm can be entered in SMON's Event Log.

This section describes the following topics:

SMON Devices

SMON provides monitoring capabilities for Avaya Inc.'s network devices that support the SMON extensions of the RMON standard.

For Avaya C460 Devices, SMON monitoring capabilities can be activated by purchasing an SMON license from Avaya Inc.

Filtering Options

SMON tools provide different methods of filtering the information displayed on the screen. These methods include:

- **Specific Filtering**
- **TopN Filtering**

Specific Filtering

Specific filtering options provide the ability to specify the switches, VLANs, ports, hosts, subnets, or protocols for which you want to view SMON information.

TopN Filtering

TopN filtering provides the ability to filter information based on the amount of a particular type of traffic being monitored. When using TopN filtering, specify the number of switches, VLANs, ports, hosts, subnets, or protocols for which you want to view SMON information. Then select a statistic which will be used as the basis for the filtering.

Using TopN filtering you can, for example, view information on only the top 5 most active ports, or on the 8 switches generating the most error traffic.

TopN filtering is powerful in that it allows you to focus on the information that is important to you. For information on implementing TopN filtering, refer to "Using the Define TopN Filter Dialog Box" on page 86.

Device SMON Tools

The following sections describe the Device SMON tools for Avaya C460:

- **Switch Statistics Overview** - Describes how the C460 provides detailed information on traffic passing through the switch fabric.
- **Port Statistics Overview** - Describes how the C460 provides detailed information on port traffic to help determine the precise cause of a problem.
- **Extended Port Statistics Overview** - Describes how the C460 provides detailed information on the types of traffic on a specific port.
- **VLAN Statistics Overview** - Describes how the C460 provides detailed information on switch traffic associated with a VLAN.
- **Alarms and Events Overview** - Describes how the C460 provides notification of user defined events that help monitor a rise or fall of the rate of specified packets on selected ports.

Switch Statistics Overview

The Switch Statistics tool provides details of the traffic passing through the switch fabric and allows you to detect problems on the switch. Once a problem has been detected, you can use VLAN or Port Statistics to determine more precisely the cause of the problem.

The display includes two sections:

- Pie charts and gauges showing traffic breakdown.
- A traffic graph that describes the characteristics of the traffic passing through the device.

You can use the Switch Statistics tool for the following purposes:

- Gaining an overall view of the switched traffic over a specific time period. This can help in discovering problems and analyzing traffic trends.
- Discovering whether the device is being utilized efficiently or not.
- Monitoring the load distribution among switches.
- Detecting a large number of broadcast messages sent. This indicates there may be a problem with a station on the network.
- Treating any variable with abnormal behavior as an issue that should be investigated further using other SMON tools.

In general, the Switch Statistics tool can help you spot problems that only become apparent from a high-level view over time. By periodically viewing Switch Statistics, you can detect normal and abnormal behavior of the specific switch configuration.

SMON collects and displays all information in real-time. In addition, information collected during a session can be saved in a report. For more information on using the Switch Statistics tool, refer to Chapter 3, Using Switch Statistics.

Port Statistics Overview

The Port Statistics tool measures the traffic travelling through each port on the selected device. For each port, SMON summarizes the traffic, such as packets into the device and packets from the device. You can sort the display by port name or by any of the packet types. You can see, for example, the ports generating the most errors.

If you notice that a particular port displays a disproportionate amount of errors, this may suggest that a device connected to the port is responsible for the problem.

You select the most active ports by using a rate base. SMON measures the rate base for all the ports to find the most active ports and then displays these ports and their statistics. This process is called Port TopN.

Using the Port Statistics tool in conjunction with VLAN Statistics and Switch Statistics makes it straightforward to discover the cause of a problem. For example, using Switch Statistics you may discover that there are too many errors on a specific switch. You could then use Port Statistics to help indicate the port from which the problem originates. For more information on using the Port Statistics tool, refer to Chapter 4, Using Port Statistics.

Extended Port Statistics Overview

The Extended Port Statistics tool measures the traffic travelling through a specific port. SMON shows details of the traffic on the port, including packet types and error types.

If you notice that a particular port displays a disproportionate amount of errors, Extended Port Statistics can help you identify the type of error occurring most often. This can help you pinpoint the cause of the problem. For more information on using the Extended Port Statistics tool, refer to Chapter 5, Using Extended Port Statistics.

VLAN Statistics Overview

The VLAN Statistics tool measures the switched traffic travelling through VLANs on the selected switch. A VLAN consists of stations connected logically rather than physically. A VLAN can be used, for example, to distribute network resources by department, even if the department's stations are not all located in the same area. Therefore, a VLAN can incorporate stations from different devices.

By comparing the load of each VLAN you can discover which VLANs are:

- Utilizing their full capacity.
- Under capacity.
- Over-extended and probably causing a degradation in performance to the users.

VLAN Statistics represents the information as a horizontal bar chart. Using this tool in conjunction with Port Statistics and Switch Statistics makes it straightforward to discover the cause of a problem. For example, using VLAN Statistics you may discover that there are too many broadcast errors on a specific VLAN. You could then use Port Statistics to help indicate the port from which the problem originates. For more information on using the VLAN Statistics tool, refer to Chapter 6, Using VLAN Statistics.

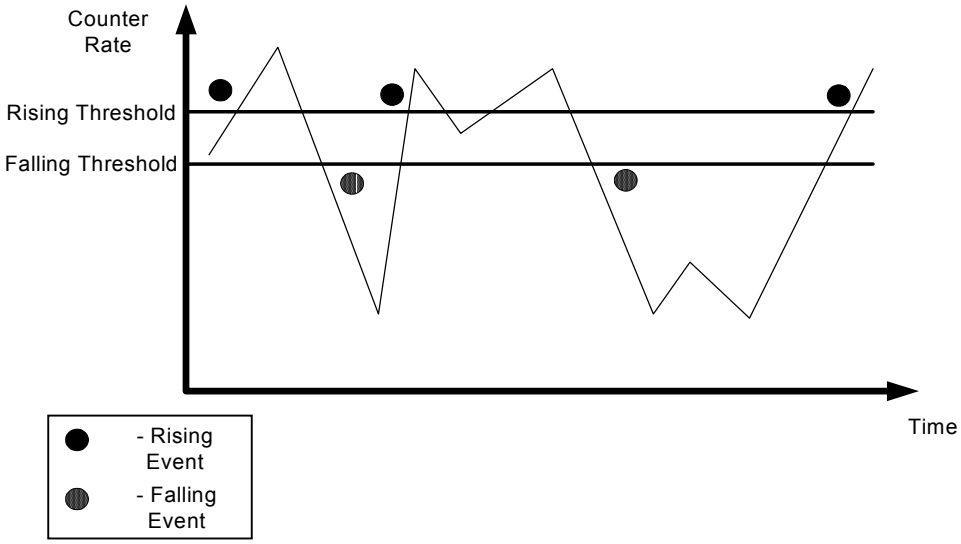
Alarms and Events Overview

The Alarms and Events tool reports when a specified counter on selected ports, or on a device, cross user defined thresholds. The Alarm Wizard provides a simple method for defining upper and lower thresholds of a counter on selected ports or on the device. This definition of the thresholds is an Alarm.

An event is the crossing of a defined threshold in the direction it was defined. For example, a Rising Event is when the rate of a specified counter on a selected port rises above the defined Rising (upper) Threshold. A Falling Event is when the rate of a specified counter on a selected port falls below the defined Falling (lower) Threshold.

The following figure shows the scheme used to generate events.

Figure 1-1. Events Overview



The first event is a Rising Event, caused by the counter rate rising above the Rising Threshold. The second event is a Falling Event, caused by the counter rate falling below the Falling Threshold. The third event is a Rising Event. Note, that although the rate falls below the Rising Threshold and then rises above it again, no event is generated. A new Rising Event can only be generated **after** the rate falls below the Falling Threshold. Similarly, after the fourth event, although the rate rises above the Falling Threshold and then falls below it again, no event is generated. A new Falling Event can only be generated **after** the rate rises above the Rising Threshold.

If you want to be informed of the rise or fall of the rate of a particular type of packet on a port, you could use the Alarm Wizard to define thresholds for the packet type on the port. You could then specify whether an event causes a trap to be sent to the device's manager, or is listed in SMON's Device Event Log, or both.

If you suspect a problem on a port, you can use Alarms and Events to notify you when a problem occurs. You could then use the Port History tool to identify the duration and frequency of the problem. This can help you locate the cause of the problem. For more information on using the Alarms and Events tool, refer to Chapter 7, Using Alarms and Events.

AnyLayer SMON Tools

The following sections describe the AnyLayer SMON tools for Avaya C460:

- **Protocol Distribution Overview** - Describes how the C460 provides detailed information on protocol traffic passing through the router module.
- **DSCP Overview** - Describes how the C460 provides detailed information on DSCP tagged traffic passing through the router module.

Protocol Distribution Overview

Protocol Distribution provides you with details about the protocols routed by an Avaya C460 routing module, and tracks the distribution of traffic through the device among various network and application layer protocols. Protocol Distribution collects all information in real-time, and displays it in a variety of powerful and easy to use graphic formats.

Protocol Distribution stores all data recently collected from the device. Protocol Distribution also allows you to save collected information in reports. You can learn what is normal and abnormal behavior for your specific network by viewing the reports and analyzing changes in your network's traffic. This can help you discover problems in your network configuration. In general, the Protocol Distribution tool can help you see things that become apparent over time from a high-level view. For more information on C460 implementation of Protocol Distribution, refer to Chapter 9, Using Protocol Distribution and DSCP Statistics.

DSCP Overview

Protocol Distribution for the Avaya C460 router modules includes monitoring of DSCP tagged traffic. DSCP is an extension of IP which provides a method of encoding QoS (Quality of Service) information in the IP header of traffic. This enables you to change the priority of packets to conform to standards for applications such as Voice over IP. Protocol Distribution for Avaya C460 router modules provides graphical representations of IP traffic with non-zero DSCP headers and IP traffic with zero DSCP headers.

A DSCP value between 0 and 63 is added to the IP header of data packets. For more information on the implementation of DSCP, refer to "Viewing DSCP Statistics" on page 72.

2 Using the Device SMON

This chapter provides information about SMON for Avaya C460 Devices, and contains the following sections:

- **Accessing Avaya C460 SMON** - Instructions on accessing the Device SMON window.
- **The Device SMON User Interface** - A detailed description of the user interface for Avaya C460 SMON.
- **Working with Device SMON Tools** - Techniques for using Device SMON more effectively.

Accessing Avaya C460 SMON

To access SMON for the Avaya C460, click the **Device SMON** tab in the Avaya C460 Manager.

The Device SMON User Interface

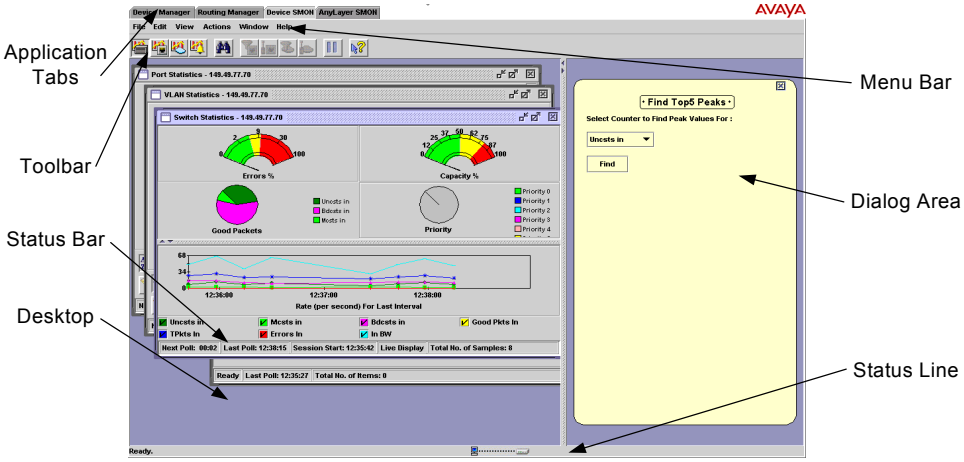
The user interface consists of the following elements:

- **Application Tabs** - Tabs for switching between the different views of the Avaya C460 Device.
- **Menu Bar** - Menus for accessing Device SMON functions.
- **Device SMON Toolbar** - Buttons providing shortcuts to important functions in Device SMON tools.
- **Dialog Area** - A resizeable window where all dialog boxes appear.
- **Desktop** - A resizeable window where Device SMON windows are displayed.

- **Status Bar** - An area at the bottom of each application window where information about the current application is displayed.
- **Status Line** - An area at the bottom of the Device SMON window where the communication status between Avaya C460 SMON and the Avaya C460 Device is displayed.

The figure below shows the user interface, with its various parts labeled.

Figure 2-1. The Avaya C460 SMON User Interface



Application Tabs

The Application Tabs provide a method for selecting the view of the device.

To switch to the device management view of the Avaya C460, click **Device Manager**. The Avaya C460 Device Manager opens.

To switch to the Device SMON view of the Avaya C460, click **Device SMON**. Avaya C460 SMON opens.

To switch to the Routing Manager view of the Avaya C460, click **Routing Manager**. Avaya C460 Routing Manager opens.

Device SMON Toolbar

The toolbar provides shortcuts to the main Device SMON functions and tools. The following table describes the buttons on the toolbar and lists the equivalent menu options.

Table 2-1. Toolbar Buttons

Button	Description	Menu
	Activates the Switch Statistics tool.	**View > Switch Statistics**
	Activates the Port Statistics tool.	**View > Port Statistics**
	Activates the VLAN Statistics tool.	**View > VLAN Statistics**
	Opens the Alarms Table.	**Tools > Alarms Table**
	Searches for a specific item. For more information, refer to "Using the Find Dialog Box" on page 83.	**Edit > Find**
	Selects a specific list of ports for display and analysis.	**Actions > Define Port Filter**
	Activates/deactivates the filter specified in Define Port Filter.	**Actions > Activate Port Filter**
	Selects a specific list of VLANs for display and analysis.	**Actions > Define VLAN Filter**
	Activates/Deactivates the filter specified in Define VLAN Filter.	**Actions > Activate VLAN Filter**
	Temporarily stops and then restarts collection of SMON data. When the collection of SMON data is paused, the background of the chart appears white.	**Actions > Pause**
	Opens the on-line help.	**Help > Help On**

If a tool is not active, clicking the corresponding Device SMON toolbar button launches the tool. If a tool is already active, clicking the corresponding Device SMON toolbar button brings the tool to the foreground. For more information about the individual tools, refer to "Device SMON Tools" on page 4.

Dialog Area

The area on the right side of the user interface is where all dialog boxes appear. This area can be resized by dragging the vertical splitter bar with the mouse. When a dialog box opens, it replaces the current dialog box open in the Dialog Area.

Desktop

The left side of the application window is the Desktop. This area can be resized by dragging the vertical splitter bar with the mouse. Device SMON application windows can be resized and minimized. Minimized windows are shown at the bottom of the Desktop.

Status Bar

The status bar provides important information about the current window. The table below describes the items found in the status bar.

*** Note:** The table below describes all the items that can appear on Avaya C460 SMON window status bars. Only some of the items appear in the status bar for each individual window.

Table 2-2. Status Bar Items

Item	Description
Graph Status	Status of the display. Possible statuses are: frozen, alive.
Last Poll	Time when the last poll was made.
Next Poll	Time remaining before the next poll.
Session Start	Date and time at which this session started.
Sort By	The active sort options (port or VLAN).
TopN	The active TopN variable, or TopN is not active.
Total Number of Items	Total number of items in the collection.
Total Number of Samples	Total number of samples in the collection.

Status Line

The status line provides important information about the communication status between the application and the Avaya C460 Device. The following table shows the messages and icons that can appear in the status line with a description of their meaning.

Table 2-3. Status Line Items

Message	Icon	Description
`Ready`		The application is ready to communicate with the device.
`Communicating`		The application is currently communicating with the device.
`Error`		The last attempted communication with the device was not successful.

Working with Device SMON Tools

The following sections describe techniques that can help you use Avaya C460 SMON tools more effectively. The topics include:

- **Mouse Actions** - Information on the application's response to various mouse actions.
- **Using Dialog Box Options** - Instructions on using the dialog box options.
- **Generating Reports** - Instructions on how to generate reports.
- **Managing Windows** - Instructions on how to manage Device SMON windows.

Mouse Actions

The mouse actions that can be performed in Avaya C460 SMON windows allow you added flexibility when using the applications. The table below describes some of the mouse actions available in some of the SMON applications.

Table 2-4. Mouse Actions

Action	Description
Movement on a graph, bar, or pie	The Info Box is displayed.
Double-click in a graph	The graph freezes and is compressed to show all of the traffic on the device from the time the application was opened until the present.
Press **SHIFT** and select a portion of the graph using the mouse	The graph freezes, zooms in, and shows only the portion of the graph that was selected.
Left-click in a graph	Unfreezes the graph.

Using Dialog Box Options

Information entered in a dialog box is not saved until you click the **Apply** button. If you want to undo all changes made to the information in the dialog box, click **Undo**. The information in the dialog box reverts to what it was when the dialog box was first opened. If you have already sent information to the device from the dialog box and you click **Undo**, the information in the dialog box will revert to what it was when it was last saved.

*** Note:** When clicking **Undo**, the application does not poll the device for information. It is therefore possible that the dialog box may not reflect the true state of the device.

Generating Reports

SMON allows you to produce two types of reports:

- **Report Now**
- **Auto Report**

Generated reports are text files that can be imported into spreadsheets such as Excel, and database programs such as Access. The reports can be generated in a tab delimited format or a comma separated format. When a report is generated, it is saved to the directory specified in the Reports Directory field in the General Options dialog box.

Data in a Report Now includes only the statistics collected during the last polling interval.

For more information on selecting a format and a default directory for reports, refer to "Using the Options Dialog Box" on page 74.

For more information on generating a Report Now, refer to "Using the Report Now Dialog Box" on page 81. For more information on generating Auto Reports, refer to "Using the Auto Report Dialog Box" on page 82.

Managing Windows

Device SMON enables you to manage open windows easily.

To cascade all open windows, select **Window > Cascade**.

To bring the next window in the list to the front, select **Window > Next**.

To bring the previous window in the list to the front, select **Window > Previous**.

To close all windows, select **Window > Close All**.

To bring a window in the list to the front, select **Window >** *Window Name*, where *Window Name* is the name of the window you want to view.

3 Using Switch Statistics

Switch Statistics provides you with detailed information about the traffic passing through a switch. For a detailed overview of Switch Statistics, refer to "Switch Statistics Overview" on page 5.

This section discusses the following topics:

Accessing the Switch Statistics Window

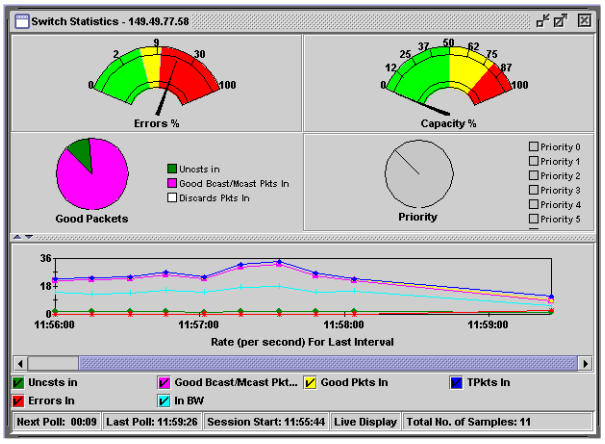
To access the Switch Statistics window:

Click  .

Or

Select **File > New > Switch Statistics**. The Switch Statistics window opens.

Figure 3-1. Switch Statistics Window



Switch Statistics displays information using different types of graphs:

- Gauges that show error packets and capacity.
- A pie chart that shows the ratio of Unicast, Broadcast, and Multicast packets.
- A pie chart that shows the ratio of packets by priority.
- A traffic graph section that contains line graphs describing the characteristics of the traffic traveling through the switch.

The title of the Switch Statistics window displays the Device IP Address.

The gauges, pie charts, and bar graph show data for the latest time currently visible on the traffic graph. For more information, refer to "Viewing the Switch Statistics Traffic Graph" on page 19.

You can use the gauges, pie charts, and traffic graph to view data from an earlier point in time by scrolling the traffic graph. For more information about modifying the display, refer to "Using the Options Dialog Box" on page 74. For more information on the available toolbar, status bar, and mouse movement options, refer to "Working with Device SMON Tools" on page 14.

Viewing the Switch Statistics Gauges and Pie Charts

The gauges at the top of the window display the following information:

Table 3-1. Gauge Variables in Switch Statistics

Variable	Description
Errors	Displays the percentage of packets that contain errors going through the device on a logarithmic scale. If this percentage is high, this indicates that there may be a problem.
Capacity	Displays the proportion of traffic in relation to the device's configured capacity, as a percentage. If the capacity used nears the device's total capability, this indicates there may be a problem.

The pie charts at the top of the window display the following information:

Table 3-2. Pie Chart Variables in Switch Statistics

Variable	Description
Unicasts in	Displays the percentage of unicast packets entering the device. On most networks, the unicast packets should constitute the vast majority of the pie graph. If non-unicast packets begin to increase, this indicates there may be a problem.
Bdcsts in	Displays the percentage of broadcast packets entering the device.
Mcsts in	Displays the percentage of multicast packets entering the device.
Priority *x* Packets	Displays the percentage of packets of priority *x* entering the device, where *x* has a value from 0 to 7.

SMON updates these gauges and pie charts in real-time according to the specified sampling interval. By viewing the relationships among these two variables, you can learn a lot about the general behavior of the switch.

*** Note:** If contact with the device is lost, the graphs will display the last data received until communications are restored.

Viewing the Switch Statistics Traffic Graph

The lower portion of the Switch Statistics window is a traffic graph. The traffic graph displays selected variables as a line graph, in real-time. To select the color coded variables you want graphed, use the check boxes under the traffic graph.

The following table provides a list of the available traffic variables and their descriptions.

Table 3-3. Traffic Variables in Switch Statistics

Variable	Description
Bdcsts in	Good broadcast packets entering into the switch.
Errors In	Error packets entering the switch.
Good Pkts In	Good packets entering the switch.
In BW	Total number of kilobits entering the switch.
Mcsts in	Good multicast packets entering the switch.

Table 3-3. Traffic Variables in Switch Statistics (Continued)

Variable	Description
TPkts In	Total packets entering the switch.
Uncsts in	Good unicast packets entering the switch.

SMON continuously monitors statistics for all available Switch Statistics traffic variables, even those that are not currently selected. For information on finding the 5 highest peaks of traffic, refer to "Using the Find Top5 Peaks Dialog Box" on page 87.

The X axis of the graph represents time. The scale on the X axis can be changed using the Samples Per Screen field in the Switch Options dialog box. For more information, refer to "Using the Options Dialog Box" on page 74.

The units of the Y axis for all variables are packets. The scale on the Y axis depends on the maximum value among all of the variables. If the spread of values is wide, the graphs of variables with small values may not be visible. In this case, use the logarithmic traffic display to produce better results. For more information, refer to "Logarithmic Display" on page 78.

Comparing the traffic graphs to the meters can often point you in the right direction for locating a problem. For example, the pie chart may show an abnormal amount of non-unicast packets, while the bandwidth usage shown in the traffic graph has increased significantly. This may suggest that one of the stations attached to the switch is generating the non-unicast packets. By using VLAN Statistics you can locate the VLAN where the problem originates. By using Port Statistics you can locate the port to which the suspected station is attached.

*** Note:** All counters are in packets except counters that measure bandwidth, which are in kilobits per second (Kbps).

4 Using Port Statistics

Port Statistics allows you to see the data passing through each port and LAG connected to the switch. For a detailed overview of Port Statistics, refer to "Port Statistics Overview" on page 6.

This section discusses the following topics:

Accessing the Port Statistics Window

To access the Port Statistics window:

Click  .

Or

Select **File > New > Port Statistics**. The Port Statistics application opens.

To select a set of statistics to display, click one of the option buttons on the lower right-hand corner of the window. The statistics sets are:

- **Packets** - Counters for selected packet types for each port and LAG.
- **Bandwidth** - The rate at which traffic is entering and exiting each port and LAG.
- **Utilization** - The utilized capacity of each port and LAG.

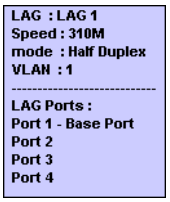
The variables relevant to the selected set of statistics appear under the graph. Check the variables you want displayed. Statistics for the checked variables are displayed as bar graphs.

Using The Port Statistics Window

The Port Statistics window is organized as follows:

- The title of the Port Statistics window shows the IP address of the device.
- The X axis represents packets or percentage for Utilization.
- The Y axis represents ports and LAGs. Each row on the graph corresponding to a port or LAG is labeled on the Y axis with a port number, LAG number, or with the user defined name for a port.
- Link Aggregation Groups (LAGs) are displayed. These are a group of ports serving as one logical link. When referencing the LAG's information box (place your cursor over the LAG bar), each port within the LAG appears (refer to the figure below). In addition, the speed of the LAG is the sum of the speed of all the ports within the LAG.

Figure 4-1. LAG Information Box



To display user defined names for ports, select **View > User Names**. A checkmark appears next to User Names, and the user defined names for ports are displayed in the Port Statistics window.

To hide user defined names for ports, select **View > User Names**. The checkmark next to User Names disappears, and port numbers are displayed in the Port Statistics window.

*** Note:** For high-speed ports with large polling intervals, bandwidth and utilization counters may be inaccurate.

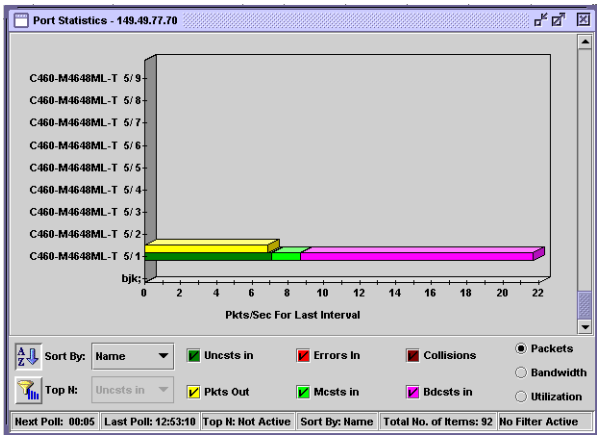
For more information about modifying the display, and the available toolbar, status bar, and mouse movement options, refer to "Working with Device SMON Tools" on page 14.

This section provides information about the following topics:

Viewing Packet Statistics

The following graphic shows the Avaya C460 Port Statistics window with Packet Statistics displayed.

Figure 4-2. Port Statistics Window - Packets



The following table provides a list of the variables available in the Port Statistics - Packets window.

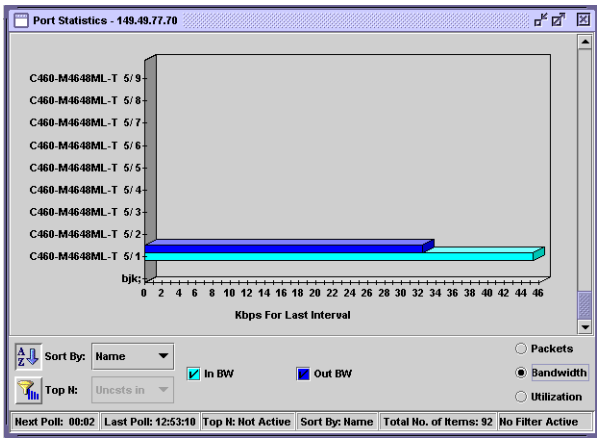
Table 4-1. Packet Statistics Variables

Variable	Description
Bdcsts In	The number of good broadcast packets entering the switch.
Collisions	The number of collisions occurring on the port or LAG.
Errors in	The number of error packets filtered out by the switch.
Pkts Out	The number of good packets leaving the switch.
Mcsts in	The number of good multicast packets entering the switch.
Uncsts Pkts in	The number of good unicast packets entering the switch.

Viewing Bandwidth Statistics

The following graphic shows the Avaya C460 Port Statistics window with Bandwidth Statistics displayed.

Figure 4-3. Port Statistics Window - Bandwidth



The following table provides a list of the variables available in the Port Statistics - Bandwidth window.

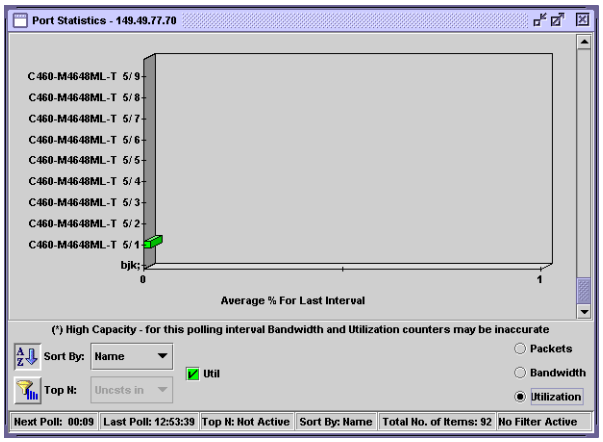
Table 4-2. Bandwidth Statistics Variables

Variable	Description
In BW	The rate at which traffic is entering the port or LAG.
Out BW	The rate at which traffic is exiting the port or LAG.

Viewing Utilization Statistics

The following graphic shows the Avaya C460 Port Statistics window with Utilization Statistics displayed.

Figure 4-4. Port Statistics Window- Utilization



The following table provides a list of the variables available in the Port Statistics - Utilization window.

Table 4-3. Utilization Statistics Variables

Variable	Description
Util	The percentage of the port or LAG's capacity currently being utilized.

Selecting Ports to Display

By default, information from all ports and LAGs is displayed in the Port Statistics window. You can limit information being displayed to specific ports using Port, VLAN, and TopN filters. In addition, you can sort the display. For information on sorting the display, refer to "Sorting the Port Display" on page 30.

This section provides information about the following topics:

- **Port Filtering**
- **VLAN Filtering**
- **TopN Port Filtering**

Port Filtering

You can filter the ports and LAGs displayed in the Port Statistics window. Only selected ports are displayed in the Port Statistics window. This makes it easier to concentrate on specific ports and LAGs in the network.

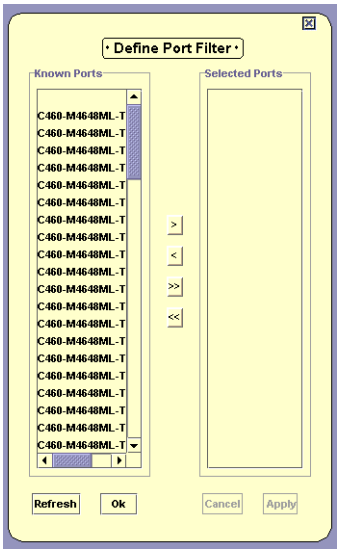
To open the Define Port Filter dialog box:

Click  .

Or

Select **View > Define Port Filter**. The Define Port Filter dialog box opens.

Figure 4-5. Define Port Filter Dialog Box



To add ports to the Selected Ports list:

Select ports and LAGs from the Known Ports list and click **>**.

Or

Double-click ports and LAGs in the Known Ports list. The selected ports and LAGs appear in the Selected Ports list.

To select all ports and LAGs, click **>>**. All ports and LAGs are added to the Selected Ports list.

To remove ports and LAGs from the Selected Ports list:

Select ports and LAGs in the Selected Ports list and click **<**.

Or

Double-click ports and LAGs in the Selected Ports list. The selected ports and LAGs are removed from the Selected Ports list.

To remove all items from the Selected Ports list, click **<<**. All ports and LAGs are removed from the Selected Ports list.

To refresh the Known Ports list, click **Refresh**.

To apply the port filter, click **Apply**. The Port Statistics information is filtered.

To define the port filter without applying it, click **OK**.

To toggle the port filter:

Click  .

Or

Select **View > Activate Port Filter**.

VLAN Filtering

You can filter the ports and LAGs displayed in the Port Statistics window by VLAN. Only ports that are members of the selected VLANs are displayed in the Port Statistics window. This makes it easier to concentrate on specific VLANs in the network.

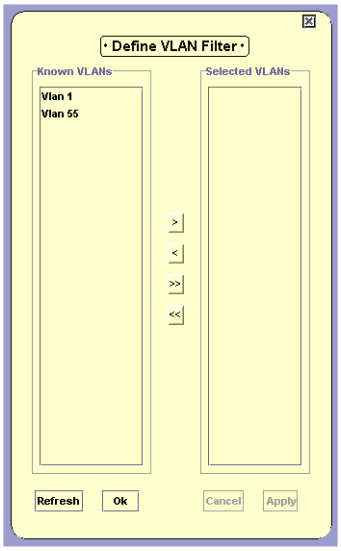
To open the Define VLAN Filter dialog box:

Click  .

Or

Select **View > Define VLAN Filter**. The Define VLAN Filter dialog box opens.

Figure 4-6. Define VLAN Filter Dialog Box



To add VLANs to the Selected VLANs list:

Select VLANs from the Known VLANs list and click **>**.

Or

Double-click VLANs in the Known VLANs list. The selected VLANs appear in the Selected VLANs list.

To select all VLANs, click **>>**. All VLANs are added to the Selected VLANs list.

To remove VLANs from the Selected VLANs list:

Select VLANs in the Selected VLANs list and click **<**.

Or

Double-click VLANs in the Selected VLANs list. The selected VLANs are removed from the Selected VLANs list.

To remove all items from the Selected VLANs list, click **<<**. All VLANs are removed from the Selected VLANs list.

To refresh the Known VLANs list, click **Refresh**.

To apply the VLAN filter, click **Apply**. The Port Statistics information is filtered.

To define the VLAN filter without applying it, click **OK**.

To toggle the VLAN filter:

Click  .

Or

Select **View > Activate VLAN Filter**.

TopN Port Filtering

TopN filtering enables SMON to display only the items with the heaviest traffic. The TopN filter produces a report for the 1-15 (*N*) most active items on the network.

SMON selects the TopN items by a rate base which you select from the pull-down listbox in the Port Statistics window. SMON measures the rate base for all the items to find the TopN items and then displays these items and their statistics.

For information on defining the number of items to display using TopN filtering, refer to "Port/VLAN Tab" on page 79.

To activate the TopN filter, click  at the bottom of the Port Statistics window. To deactivate the TopN filter, click  at the bottom of the Port Statistics window.

To select a rate base, select a TopN criteria from the TopN pull-down listbox at the bottom of the Port Statistics window.

Sorting the Port Display

You can sort the display by the port name or any of the counters available for the port.

To sort the display:

1. Click  .
2. Select a sorting criterion from the Sort By pull-down listbox. The display is sorted by the selected criteria.

When sorting by name, the bars appear in ascending order from bottom to top. When sorting by packets, the bars appear in descending order (most traffic at the bottom, least traffic at the top).

5 Using Extended Port Statistics

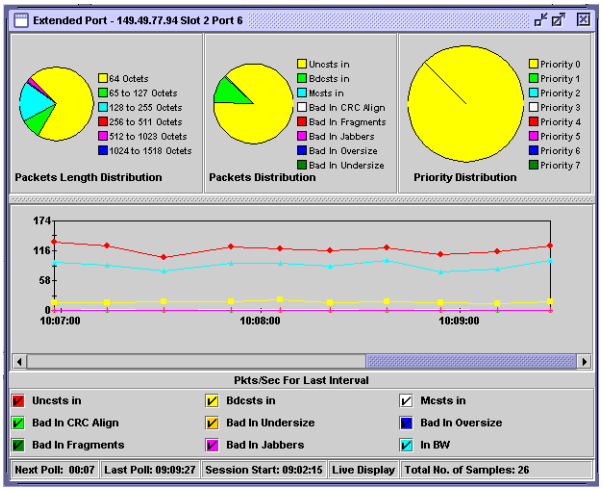
Extended Port Statistics allows you to see details about the data passing through a specific port or LAG connected to the switch. For a detailed overview of Extended Port Statistics, refer to "Extended Port Statistics Overview" on page 6.

This section discusses the following topics:

Accessing the Extended Port Statistics Window

To access the Extended Port Statistics window, double-click the port or LAG bar in the Port Statistics window. The Extended Port Statistics application opens.

Figure 5-1. Extended Port Statistics



Extended Port Statistics displays information using two types of graphs:

- Pie charts that shows the ratio of different types of packets.
- A traffic graph section that contains line graphs describing the characteristics of the traffic traveling through the port or LAG.

The title of the Extended Port Statistics window displays the name of the port or LAG selected.

The pie charts show data for the latest time currently visible on the traffic graph. For more information, refer to "Viewing the Traffic Graph in the Extended Port Statistics Window" on page 34.

You can use the pie charts and the traffic graph to view data from an earlier point in time by scrolling the traffic graph. For more information on the available toolbar, status bar, and mouse movement options, refer to "Working with Device SMON Tools" on page 14.

Viewing Pie Charts in the Extended Port Statistics Window

There are three pie charts at the top of the window. The leftmost pie chart displays Packets Length Distribution, the center pie chart displays Packets Distribution, and the rightmost pie chart displays Priority Distribution.

The following table provides a list of the statistics found in the Packets Length Distribution pie chart:

Table 5-1. Extended Port Statistics - Packets Length Distribution

Variable	Description
64 Octets	Displays the distribution of packets on the port with a packet length of 64 octets.
65 to 127 Octets	Displays the distribution of packets on the port with a packet length of between 65 and 127 octets.
128 to 255 Octets	Displays the distribution of packets on the port with a packet length of between 128 and 255 octets.
256 to 511 Octets	Displays the distribution of packets on the port with a packet length of between 256 and 511 octets.
512 to 1023 Octets	Displays the distribution of packets on the port with a packet length of between 512 and 1023 octets.
1024 to 1518 Octets	Displays the distribution of packets on the port with a packet length of between 1024 and 1518 octets.

The following table provides a list of the statistics found in the Packets Distribution pie chart:

Table 5-2. Extended Port Statistics - Packets Distribution

Variable	Description
Bad In CRC Align	Displays the distribution of packets entering the port with a CRC alignment error.
Bad In Fragments	Displays the distribution of fragmented packets entering the port.
Bad In Jabbers	Displays the distribution of jabber packets entering the port.
Bad In Oversize	Displays the distribution of oversize packets entering the port.
Bad In Undersize	Displays the distribution of undersize packets entering the port.
Bdcsts in	Displays the distribution of broadcast packets entering the port.
Mcsts in	Displays the distribution of multicast packets entering the port.
Uncsts in	Displays the distribution of unicast packets entering the port. On most networks, the unicast packets should constitute the vast majority of the pie graph. If non-unicast packets begin to increase, there may be a problem.

The following table provides a list of the statistics found in the Priority Distribution pie chart:

Table 5-3. Extended Port Statistics - Priority Distribution

Variable	Description
Priority 0	Displays the distribution of packets of priority 0 entering the port.
Priority 1	Displays the distribution of packets of priority 1 entering the port.
Priority 2	Displays the distribution of packets of priority 2 entering the port.
Priority 3	Displays the distribution of packets of priority 3 entering the port.
Priority 4	Displays the distribution of packets of priority 4 entering the port.

Table 5-3. Extended Port Statistics - Priority Distribution (Continued)

Variable	Description
Priority 5	Displays the distribution of packets of priority 5 entering the port.
Priority 6	Displays the distribution of packets of priority 6 entering the port.
Priority 7	Displays the distribution of packets of priority 7 entering the port.

SMON updates these pie charts in real-time according to the specified sampling interval. By viewing the relationships among these variables, you can learn a lot about the traffic on the port.

*** Note:** If contact with the device is lost, the graphs will display the last data received until communications are restored.

Viewing the Traffic Graph in the Extended Port Statistics Window

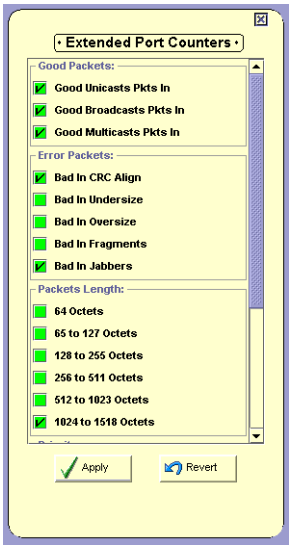
The lower portion of the Extended Port Statistics window is a traffic graph. The traffic graph displays selected variables as a line graph, in real-time.

The X axis of the graph represents time. The units of the Y axis for all variables are packets. The scale on the Y axis depends on the maximum value among all of the variables. If the spread of values is wide, the graphs of variables with small values may not be visible. In this case, use the logarithmic traffic display to produce better results (refer to "Logarithmic Display" on page 78).

To select a set of statistics to display:

1. Select **Actions > Define Extended Port Counters**. The Extended Port Counters dialog box opens.

Figure 5-2. Extended Port Counters Dialog Box



2. Check the checkboxes next to the counters you want displayed in the traffic graph.

*** Note:** A maximum of 9 counters can be displayed in the traffic graph.

3. Click **Apply**. The selected counters appear under the traffic graph.

4. At the bottom of the Extended Port Statistics window, check the variables you want displayed. Statistics for the checked variables are displayed as line graphs.

SMON continuously monitors statistics for all available Extended Port Statistics traffic variables, even those that are not currently selected. For information on finding the 5 highest peaks of traffic, refer to "Using the Find Top5 Peaks Dialog Box" on page 87.

The following table lists the counters available for display in the Extended Port Statistics traffic graph.

Table 5-4. Extended Port Statistics Counters

Variable	Description
Uncsts In	The number of unicast packets entering the port. On most networks, the unicast packets should constitute the vast majority of the pie graph. If non-unicast packets begin to increase, this indicates there may be a problem.
Mcsts In	The number of multicast packets entering the port.
Bdcsts In	The number of broadcast packets entering the port.
Bad In CRC Align	The number of packets entering the port with a CRC alignment error.
Bad In Undersize	The number of undersize packets entering the port.
Bad In Oversize	The number of oversize packets entering the port.
Bad In Fragments	The number of fragmented packets entering the port.
Bad In Jabbers	The number of jabber packets entering the port.
64 Octet	The number of packets on the port with a packet length of 64 octets.
65 to 127 Octets	The number of packets on the port with a packet length of between 65 and 127 octets.
128 to 255 Octets	The number of packets on the port with a packet length of between 128 and 255 octets.
256 to 511 Octets	The number of packets on the port with a packet length of between 256 and 511 octets.
512 to 1023 Octets	The number of packets on the port with a packet length of between 512 and 1023 octets.
1024 to 1518 Octets	The number of packets on the port with a packet length of between 1024 and 1518 octets.
Priority *x*	The number of packets of priority *x* entering the device, where *x* has a value between 1 and 8.
In BW	The rate at which traffic is entering the port.

6 Using VLAN Statistics

VLAN Statistics displays detailed statistics for each VLAN. These statistics can help you maintain proper VLAN configuration. They can also help you pinpoint problems you may discover using Switch Statistics. For a detailed overview of VLAN Statistics, refer to "VLAN Statistics Overview" on page 6.

*** Note:** The statistics collected for each VLAN only include the packets that are sent to and from stations connected to the switch fabric of the device being analyzed. Therefore, any traffic that does not pass through the switch fabric of the selected device is not included in the statistics.

This section discusses the following topics:

Accessing VLAN Statistics

To access the VLAN Statistics window:

Click  .

Or

Select **File > New > VLAN Statistics**. The VLAN Statistics application opens.

To select a set of statistics to display, click one of the option buttons on the lower right-hand corner of the window. The statistics sets are:

- **Packets** - Counters for selected packet types for each VLAN.
- **Bandwidth** - The rate at which traffic is entering and exiting each VLAN.

The variables relevant to the selected set of statistics appear under the graph. Check the variables you want displayed. Statistics for the checked variables are displayed as bar graphs.

Using the VLAN Statistics Window

The VLAN Statistics window is organized as follows:

- The title of the VLAN Statistics window displays the IP address of the device.
- The X axis relates to packets over time or total packets, depending on the display mode (refer to "Display Mode" on page 76).
- The Y axis relates to the VLAN name. Only VLANs with member ports or LAGs appear in the window. If no VLANs have been defined, the "Default" or "Generic" VLAN includes all traffic.

For more information about modifying the display, and the available toolbar, status bar and mouse movement options, refer to "Working with Device SMON Tools" on page 14.

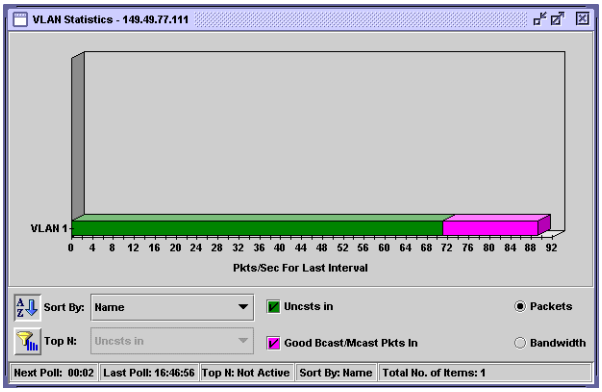
This section discusses the following topics:

- **Viewing VLAN Packet Statistics**
- **Viewing VLAN Bandwidth Statistics**
- **Selecting VLANs to Display**
- **Sorting the VLAN Display**

Viewing VLAN Packet Statistics

The following graphic displays the VLAN Packet Statistics window.

Figure 6-1. VLAN Statistics Window - Packets



The following table provides a list of the variables available in the VLAN Statistics - Packets window.

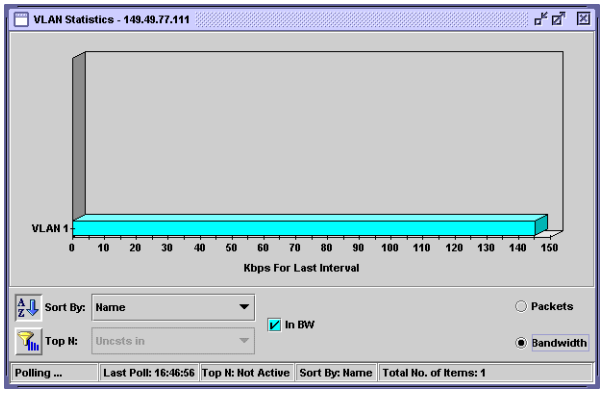
Table 6-1. VLAN Statistics Variables - Packets

Variable	Description
Good Bcast/Mcast Pkts In	The number of good non-unicast packets entering the switch.
Uncsts In	The number of good unicast packets entering the switch.

Viewing VLAN Bandwidth Statistics

The following graphic displays the VLAN Bandwidth Statistics window.

Figure 6-2. VLAN Statistics Window - Bandwidth



The following table provides a list of the variables available in the VLAN Statistics - Bandwidth window.

Table 6-2. VLAN Statistics Variables - Bandwidth

Variable	Description
In BW (Kbps)	The rate at which traffic is entering the VLAN.

Selecting VLANs to Display

By default, information from all VLANs is displayed in the VLAN Statistics window. You can limit information being displayed to specific VLANs using VLAN and TopN filters. In addition, you can sort the display. For information on sorting the display, refer to "Sorting the VLAN Display" on page 43.

VLAN Filtering

You can filter the VLANs displayed in the VLAN Statistics window by VLAN. Only selected VLANs are displayed in the VLAN Statistics window. This makes it easier to concentrate on specific VLANs in the network.

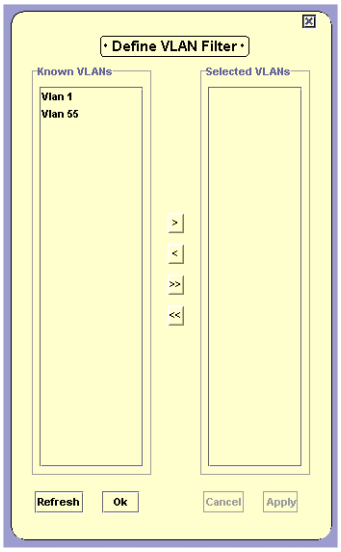
To open the Define VLAN Filter dialog box:

Click  .

Or

Select **View > Define VLAN Filter**. The Define VLAN Filter dialog box opens.

Figure 6-3. Define VLAN Filter Dialog Box



To add VLANs to the Selected VLANs list:

Select VLANs from the Known VLANs list and click **>**.

Or

Double-click VLANs in the Known VLANs list. The selected VLANs appear in the Selected VLANs list.

To select all VLANs, click **>>**. All VLANs are added to the Selected VLANs list.

To remove VLANs from the Selected VLANs list:

Select VLANs in the Selected VLANs list and click **<**.

Or

Double-click VLANs in the Selected VLANs list. The selected VLANs are removed from the Selected VLANs list.

To remove all items from the Selected VLANs list, click **<<**. All VLANs are removed from the Selected VLANs list.

To refresh the Known VLANs list, click **Refresh**.

To apply the VLAN filter, click **Apply**. The VLAN Statistics information is filtered.

To define the VLAN filter without applying it, click **OK**.

To toggle the VLAN filter:

Click  .

Or

Select **View > Activate VLAN Filter**.

TopN VLAN Filtering

TopN filtering enables SMON to display only the items with the heaviest traffic. The TopN filter produces a report for the 1-15 (*N*) most active items on the network.

SMON selects the TopN items by a rate base which you select from the pull-down listbox in the VLAN Statistics window. SMON measures the rate base for all the items to find the TopN items and then displays these items and their statistics.

For information on defining the number of items to display using TopN filtering, refer to "Port/VLAN Tab" on page 79.

To activate the TopN filter, click  at the bottom of the VLAN Statistics window. To deactivate the TopN filter, click  at the bottom of the VLAN Statistics window.

To select a rate base, select a TopN criteria from the TopN pull-down listbox at the bottom of the VLAN Statistics window.

Sorting the VLAN Display

You can sort the display by the VLAN name or any of the counters available for the VLAN.

To sort the display:

1. Click  .
2. Select a sorting criterion from the Sort By pull-down listbox. The display is sorted by the selected criteria.

When sorting by name, the bars appear in ascending order from bottom to top. When sorting by packets, the bars appear in descending order (most traffic at the bottom, least traffic at the top).

7 Using Alarms and Events

The Alarms and Events tool provides a method for defining thresholds for packet types on a port. When a threshold is crossed, a trap is sent to the device's manager, or the event is listed in SMON's Device Event Log.

This chapter explains the following topics:

- **Using the Alarms and Events Tool** - An overview explaining how to use the Alarms and Events feature.
- **Alarms Table** - A table showing the alarms defined for the device.
- **Alarm Wizard** - A wizard that enables you to add new alarms.
- **Device Event Log** - A list of events that occurred on the device.

Using the Alarms and Events Tool

To use the Alarms and Events tool:

1. Add alarms using the Alarm Wizard. For information on the Alarm Wizard, refer to "Alarm Wizard" on page 49.
2. Review, edit, and delete alarms defined for the device in the Alarms Table. For information on the Alarms Table, refer to "Alarms Table" on page 45.
3. View events in SMON's Device Event Log or in the Trap Log of Avaya MultiService Console or HP-OV NNM. For information on the SMON Device Event Log, refer to "Device Event Log" on page 57.

Alarms Table

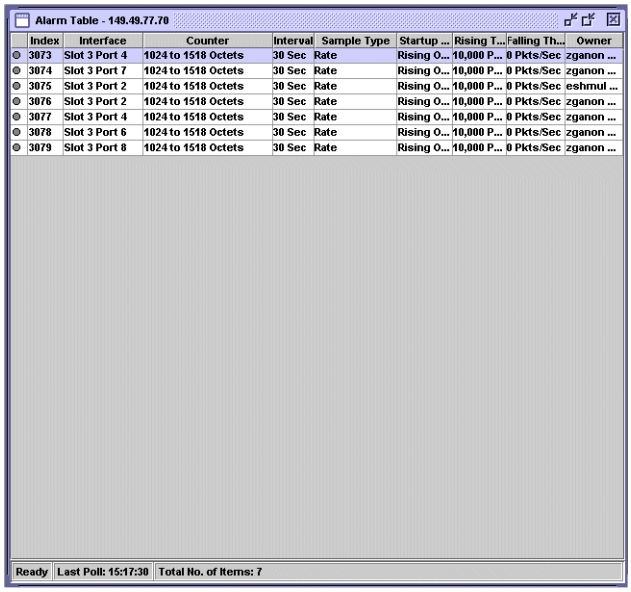
To view a table of all the alarms defined for the device:

Click  .

Or

Select **Tools > Alarms Table**. The Alarms Table opens.

Figure 7-1. Alarms Table



All the alarms defined for the device are listed in the Alarms Table.

Alarms Table Fields

The following table provides a list of the fields in the Alarms Table with their description.

Table 7-1. Alarms Table Fields

Field	Description
Index	A number identifying the alarm.
Interface	The port or LAG for which the alarm was configured.
Counter	The counter being monitored by the alarm.
Interval	The interval at which the counter is compared to the defined thresholds.

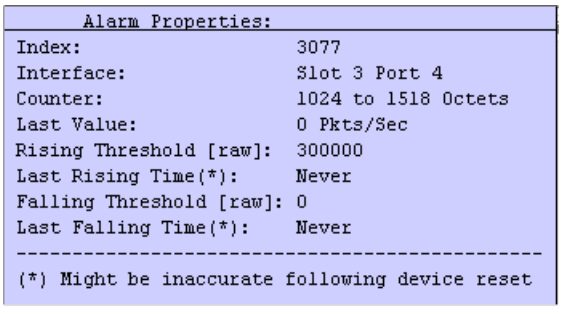
Table 7-1. Alarms Table Fields (Continued)

Field	Description
Sample Type	The method used for monitoring the variable. Possible options are: • **Rate** - The alarm uses the counter's rate in the last interval. • **Total** - The alarm uses the absolute number of the counter from the time the device was last reset. *** Note:** The Alarms and Events tool can only configure alarms using the **Rate** method. To configure alarms based on the absolute number of packets, use the CLI (Command Line Interface) or a third-party application.
Startup Alarm	The type of event that can be generated as the first event for the alarm. Possible types are: • **Rising** - The first event that can be generated must be a Rising Event. If the rate falls below the Falling Threshold before it rises above the Rising Threshold, a Falling Event is not generated. • **Falling** - The first event that can be generated must be a Falling Event. If the rate rises above the Rising Threshold before it falls below the Falling Threshold, a Rising Event is not generated. • **Rising and Falling** - The first event generated can be a Rising or a Falling Event.
Rising Threshold	The upper threshold for the counter.
Falling Threshold	The lower threshold for the counter.
Owner	The owner of the alarm. This is usually the person who created the alarm.

Tooltips

Tooltips in the Alarms and Events tool provide information about an alarm. When the cursor is held over the Index field of a row in the Alarms Table a tooltip appears.

Figure 7-2. Alarm Tooltip



The tooltip provides information about the alarm's definition. In addition, it shows the 'raw' number of packets (or octets) which will generate a Rising or Falling Event. The raw number is the actual number of packets (or octets) that must enter the port in order to generate an event. This number is equal to the defined rate times the interval.

For example, if an alarm is defined for Broadcast packets with an Interval of 15 seconds, a Rising Threshold of 1,000 packets per second and a Falling Threshold of 100 packets per second, the raw number for a Rising Event is 15,000 and for a Falling Event 1,500. If 15,000 or more Broadcast packets enter the port in a 15 second interval, a Rising Event is generated.

The following table provides a list of the fields in a tooltip with their descriptions.

Table 7-2. Tooltip Fields

Field	Description
Index	A number identifying the alarm.
Interface	The port or LAG for which the alarm was configured.
Counter	The counter being monitored by the alarm.
Last Value	The value of the counter calculated for the last interval.
Rising Threshold [raw]	The Rising Threshold expressed as the number of packets or octets in an interval.
Last Rising Time	The time of the last Rising Event.
Falling Threshold [raw]	The Falling Threshold expressed as the number of packets or octets in an interval.

Table 7-2. Tooltip Fields (Continued)

Field	Description
Last Falling Time	The time of the last Falling Event.

Editing Alarms

Alarms can be edited and deleted using the Alarms Table.

To edit an alarm, change the alarm's parameters in the Alarms Table.

To delete an alarm:

1. Select an alarm.
2. Select **Edit > Delete Alarm**. The alarm is deleted from the Alarms Table.

To save the changes to the Alarms Table, select **Edit > Apply Alarm**. All changes to the Alarm Table are saved.

To undo all unsaved changes to the Alarms Table, select **Edit > Undo Alarm**. All changes to the Alarm Table are undone.

Alarm Wizard

This section provides the information you need to use the Alarm Wizard. It contains the following topics:

- **Overview of the Alarm Wizard** - An overview of the function of the Alarm Wizard.
- **Activating the Alarm Wizard** - Instructions on how to run the Alarm Wizard.
- **Alarm Wizard Screens** - Detailed explanations about each of the steps in the Alarm Wizard.

Overview of the Alarm Wizard

The Alarm Wizard consists of several screens designed to enable you to easily define alarms for ports on the device. You can use the wizard to define an alarm for a single port or for multiple ports. When defining an alarm for more than one port, the wizard creates a separate alarm for each port.

*** Note:** A maximum of 150 alarms can be defined on a single device.

Activating the Alarm Wizard

To activate the Alarm Wizard, select **Actions > Alarm Wizard**. The Welcome screen of the Alarm Wizard opens.

Alarm Wizard Screens

This section provides detailed information on each of the Alarm Wizard's screens. To accept the default options for any screen, click **Next**. To return to an earlier screen, click **Back**. To exit the Alarm Wizard without making any changes, click **Cancel**.

The following sections describe each of the Alarm Wizard screens.

Welcome to the Alarm Wizard

Welcome to the Alarm Wizard. The Alarm Wizard provides a simple method for defining alarms for the device.

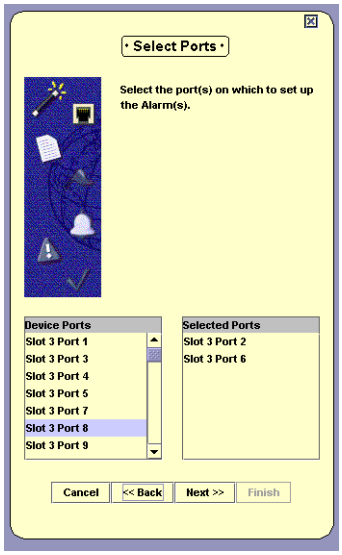
Figure 7-3. Alarm Wizard - Welcome Screen

To continue, click **Next**. The Alarm Wizard continues with the **Select Ports** screen.

Select Ports

The Select Ports screen of the Alarm Wizard allows you to select ports and LAGs to be monitored by the alarm.

Figure 7-4. Alarm Wizard - Select Ports



The ports and LAGs on the device are listed in the Device Ports list.

To select ports and LAGs to monitor, double-click a port or LAG in the Device Ports list. The selected port or LAG appears in the Selected Ports list.

To remove ports or LAGs from the Selected Ports list, double-click a port or LAG in the Selected Ports list. The selected port or LAG is removed from the Selected Ports list and appears in the Device Ports list.

When defining an alarm for more than one port, a separate alarm is created for each port.

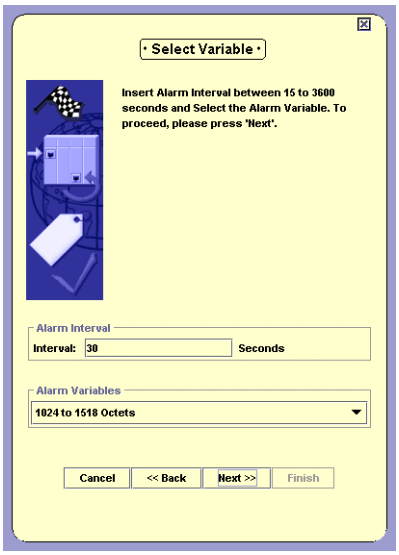
*** Note:** A maximum of 150 alarms can be defined on a device.

When you finish selecting ports and LAGs to monitor, click **Next**. The Alarm Wizard continues with the **Select Variable** screen.

Select Variable

The Select Variable screen of the Alarm Wizard enables you to select a variable to be monitored by the alarm, and the interval at which SMON gets the rate for the counter from the device.

Figure 7-5. Alarm Wizard - Select Variable Screen



Enter a number in the Alarm Interval field. This is the interval at which SMON will get the rate of the counter from the device.

Select a counter from the Alarm Counters pull-down list. This is the counter that will be monitored by the alarm.

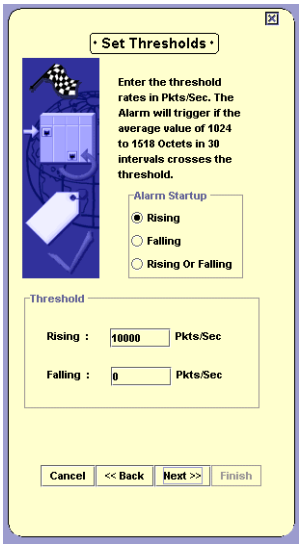
When you finish configuring the polling interval and selecting a counter to monitor, click **Next**. The Alarm Wizard continues with the **Set Thresholds** screen.

Set Thresholds

The Set Thresholds screen enables you to configure the behavior of the Alarms and Events tool when SMON is started, and to configure thresholds for the alarm.

There are two thresholds, a Rising Threshold and a Falling Threshold. If the rate of the selected counter rises above the selected Rising Threshold, an event is generated. If the rate of the selected counter falls below the selected Falling Threshold, an event is generated. For more information about Thresholds, refer to "Alarms and Events Overview" on page 7.

Figure 7-6. Alarm Wizard - Set Thresholds



To configure the behavior of the Alarms and Events tool when SMON is started, select a radio button in the Alarm Startup field. The options are:

- **Rising** - The first event that can be generated must be a Rising Event. If the rate falls below the Falling Threshold before it rises above the Rising Threshold, a Falling Event is not generated.
- **Falling** - The first event that can be generated must be a Falling Event. If the rate rises above the Rising Threshold before it falls below the Falling Threshold, a Rising Event is not generated.
- **Rising and Falling** - The first event generated can be a Rising or a Falling Event.

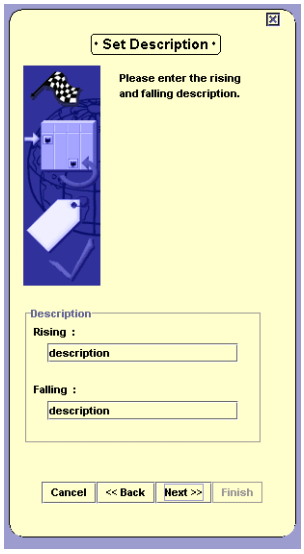
To configure the thresholds, enter values in the Rising and Falling fields. The threshold levels are in packets or octets per second.

When you finish configuring the startup behavior and thresholds, click **Next**. The Alarm Wizard continues with the **Set Description** screen.

Set Description

The Set Descriptions screen enables you to give names to the Rising and Falling Events of the alarm.

Figure 7-7. Alarm Wizard - Set Description



To configure the names of Rising and Falling Events, enter a description in the appropriate fields. These descriptions will appear in SMON's Device Event Log.

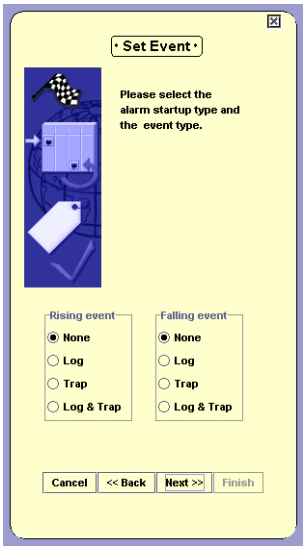
*** Note:** When configuring alarms for multiple ports, the event descriptions will be identical for the events of all the alarms being created.

When you finish configuring event descriptions, click **Next**. The Alarm Wizard continues with the **Set Event** screen.

Set Event

The Set Event screen of the Alarm Wizard allows you to determine the action SMON takes when an event occurs.

Figure 7-8. Alarm Wizard - Set Event



To configure the action SMON takes when a Rising Event occurs, select an option button in the Rising event fields. To configure the action SMON takes when a Falling Event occurs, select an option button in the Falling event fields. The possible actions are:

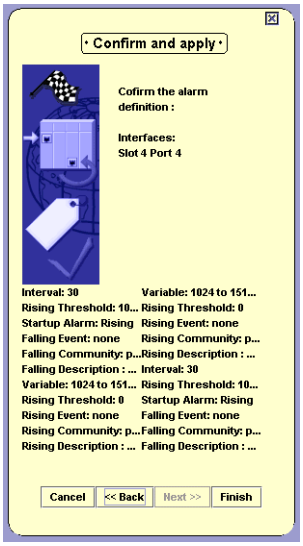
- **None** - No action is taken when the event occurs.
- **Log** - The event is recorded in SMON's Device Event Log.
- **Trap** - A trap is sent to the manager of the device. This trap can be viewed in the Trap Log in Avaya MultiService Console or HP-OV NNM.
- **Log & Trap** - The event is recorded in SMON's Device Event Log and a trap is sent to the manager of the device.

When you finish configuring event parameters, click **Next**. The Alarm Wizard continues with the **Summary** screen.

Summary

The Summary screen of the Alarm Wizard provides a summary of the options selected in the previous screens.

Figure 7-9. Summary



To make any changes to the summary information:

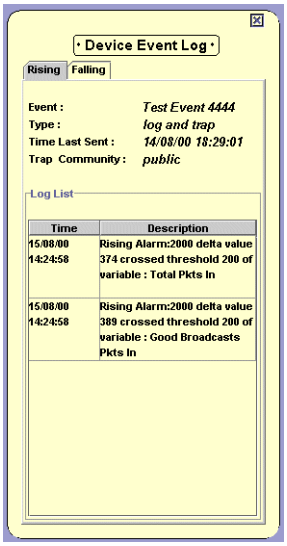
1. Click **Back** until you reach the appropriate screen.
2. Change the configuration parameters.
3. Click **Next** until you reach the Summary screen.

To create the alarm, click **Finish**. The alarm is created and appears in the Alarms Table.

Device Event Log

The Device Event Log provides a list of events that triggered alarms with an action of **Log**. To view the Event Log, select **View > Event Log**. The Device Event Log opens.

Figure 7-10. Device Event Log



The Device Event Log has two tabs, one for Rising Events and one for Falling Events. To view the Device Event Log for Rising or Falling Events:

1. Select an alarm in the Alarms Table.
2. Click the appropriate tab. The Device Event Log opens to the selected event type for the alarm.

The Device Event Log window has two parts. The upper part provides a description of the event.

The following table provides a list of the fields describing the event and their descriptions.

Table 7-3. Event Description Fields

Field	Description
Event	A user defined description of the event.
Type	The action taken by SMON. Possible actions are: • **None** - No action was taken when the event occurred. • **Log** - The event was recorded in SMON's Device Event Log. • **Trap** - A trap was sent to the manager of the device. This trap can be viewed in the Trap Log in Avaya MultiService Console or HP-OV NNM. • **log & trap** - The event was recorded in SMON's Device Event Log and a trap was sent to the manager of the device.
Time Last Sent	The latest date and time this event occurred.
Trap Community	The community of the trap recipient.

The lower part of the window is the Log List. This is a log of the selected Alarm's Events. Entries will appear in the Log List only if the Type of Event is **Log** or **log & trap**. The following table provides a list of the fields in the Log List and their descriptions.

Table 7-4. Event Log Fields

Field	Description
Time	The date and time of the event.
Description	A detailed description of the traffic that triggered the event.

8 Using AnyLayer SMON

AnyLayer SMON is used to monitor the Layer 3 protocols routed by the C460 module. This chapter provides information about AnyLayer SMON for Avaya C460 Devices, and contains the following sections:

- **Accessing AnyLayer SMON** - Instructions on accessing the AnyLayer SMON window.
- **The AnyLayer SMON User Interface** - A detailed description of the user interface for Avaya C460 AnyLayer SMON tools.

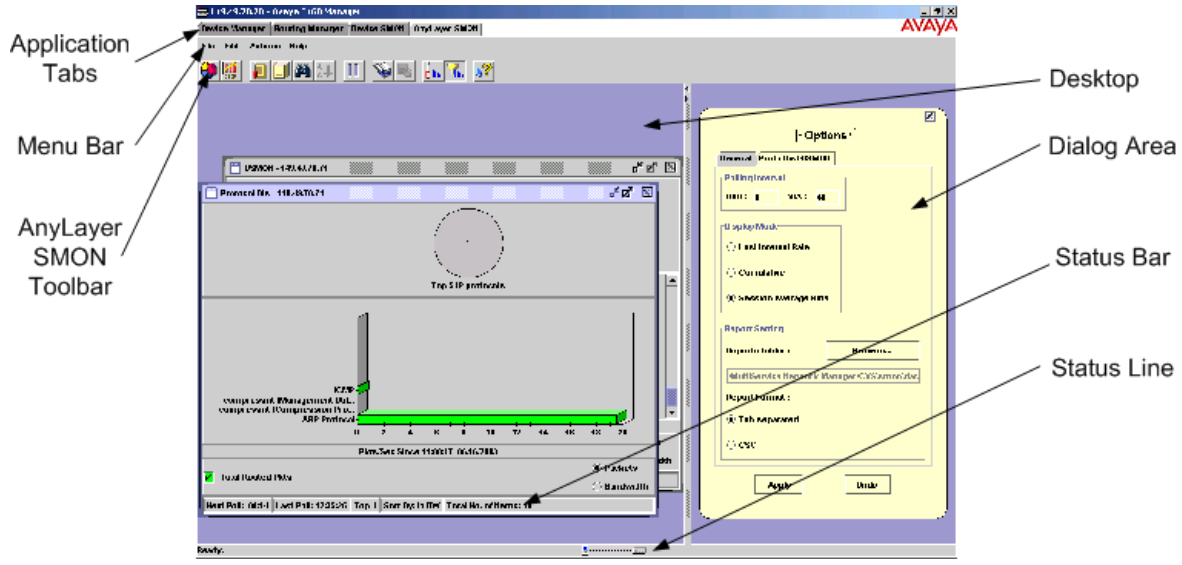
Accessing AnyLayer SMON

To access AnyLayer SMON for the Avaya C460:

1. Click the **AnyLayer SMON** tab in the Avaya C460 Manager. The tab opens.
2. Click the left-most icon on the AnyLayer SMON Toolbar to view the Protocol Distribution tool, or the icon to view the DHCP tool.

The figure below shows the user interface, with its various parts labeled.

Figure 8-1. The Avaya C460 AnyLayer SMON User Interface



The AnyLayer SMON User Interface

The user interface consists of the following elements:

- **Application Tabs** - Tabs for switching between the various views of the Avaya C460 Device.
- **Menu Bar** - Menus for accessing AnyLayer SMON functions.
- **AnyLayer SMON Toolbar** - Buttons providing shortcuts to important functions in AnyLayer SMON tools.
- **Desktop** - A resizeable window where AnyLayer SMON windows are displayed.
- **Dialog Area** - A resizeable window where all dialog boxes appear.
- **Status Bar** - An area at the bottom of each application window where information about the current tool is displayed.
- **Status Line** - An area at the bottom of the AnyLayer SMON window where the communication status between the AnyLayer SMON application and the Avaya C460 Device is displayed.

Application Tabs

The Application Tabs provide a method for selecting the view of the device.

To switch to the Avaya C460 Device Manager, click **Device Manager**. The Avaya C460 Device Manager opens.

To switch to the Routing Manager view of the Avaya C460, click **Routing Manager**. Avaya C460 Routing Manager opens.

To switch to the Device SMON view of the Avaya C460, click **Device SMON**. Avaya C460 SMON opens.

To switch to the AnyLayer SMON view of the Avaya C460, click **AnyLayer SMON**. Avaya C460 AnyLayer SMON opens.

AnyLayer SMON Toolbar

The Toolbar provides shortcuts to the main AnyLayer SMON functions and tools. The following table describes the buttons on the toolbar and lists the equivalent menu options.

Table 8-1. Toolbar Buttons

Button	Description	Menu
	Opens the Protocol Distribution window on the desktop for viewing protocol distribution statistics. For more information, refer to Chapter 9, Using Protocol Distribution and DSCP Statistics.	**File > New > Protocol Distribution Statistics**
	Opens the DSMON window on the desktop for viewing DSCP statistics. For more information, refer to "Viewing DSCP Statistics" on page 72.	**File > New > Dscp Distribution Statistics**
	Opens the General Options dialog box. For more information, refer to "Using the Options Dialog Box" on page 74.	**File > Options**
	Produces a report file for importing to a spreadsheet or database program. For more information, refer to "Using the Report Now Dialog Box" on page 81.	**File > Report Now**
	Searches for a specific item. For more information, refer to "Using the Find Dialog Box" on page 83.	**Edit > Find**
	Sorts the items in the list. For more information, refer to "Using the Sort Dialog Box" on page 88.	**Actions > Sort**
	Temporarily stops and then restarts collection of SMON data.	**Actions > Pause**
	Displays a list of protocols that can be included in the Protocol Distribution statistics. For more information, refer to "Using the Protocol Directory" on page 66.	**Actions > Protocol Directory**
	Saves changes to the device.	**Actions > Commit**
	Selects the criterion and number of items for TopN filtering. For more information, refer to "Using the Define TopN Filter Dialog Box" on page 86.	**Actions > Define Top N Filter**
	Activates/Deactivates the filter specified in Define TopN Filter.	**Actions > Activate Top N Filter**

Table 8-1. Toolbar Buttons (Continued)

Button	Description	Menu
	Opens the online-help.	**Help > Help On**

Desktop

The central area of the application window is the Desktop. This area can be resized by dragging the vertical splitter bars with the mouse. The AnyLayer SMON tool window opens on the Desktop.

Tool Tabs

The Tool Tabs provide a method for viewing the AnyLayer SMON tools. To switch to a different tool, click the appropriate Tool Tab. The selected tool opens on the Desktop.

Dialog Area

The area on the right side of the user interface is where all dialog boxes appear. This area can be resized by dragging the vertical splitter bar with the mouse. When a dialog box opens, it replaces the current dialog box open in the Dialog Area.

To apply the changes made in the dialog box, click **Apply**. The changed values are applied.

To return the settings in a dialog box to the currently configured settings, click **Revert**. The settings in the dialog box display the last applied configuration.

Status Bar

The Status Bar provides important information about the current window. The table below describes the items found in the status bar.

*** Note:** The table below describes all the items that can appear on Avaya C460 AnyLayer SMON window status bars. Only some

of the items appear in the status bar for each individual window.

Table 8-2. Status Bar Items

Item	Description
Next Poll	Time remaining before the next poll.
Last Poll	Time when the last poll was made.
Sort By	The active sort option.
TopN	The active TopN variable, or TopN is not active.
Total Number of Items	Total number of items in the collection.

Status Line

The Status Line provides important information about the communication status between the application and the Avaya C460 Device. The following table shows the messages and icons that can appear in the Status Line with a description of their meaning.

Table 8-3. Status Line Items

Message	Icon	Description
Ready		The application is ready to communicate with the device.
Communicating		The application is currently communicating with the device.
Error		The last attempted communication with the device was not successful.

9 Using Protocol Distribution and DSCP Statistics

Protocol Distribution provides a detailed analysis of how the traffic passing through an Avaya C460 with a router module is distributed among network layer and application layer protocols. For a detailed overview of Protocol Distribution, refer to "Protocol Distribution Overview" on page 9.

This chapter contains the following sections:

- **Using the Protocol Distribution Tool** - Instructions on starting Protocol Distribution, understanding the window, and using the available options.
- **Using the Protocol Directory** - Includes an overview of constant and user defined protocols, and how TCP/UDP port numbers are used, as well as instructions on starting Protocol Directory and understanding the dialog box.
- **Viewing DSCP Statistics** - Instructions on starting DSCP Statistics, understanding the window, and using the available options.

Using the Protocol Distribution Tool

To use the Protocol Distribution tool:

Click **Protocol Distribution**. The Protocol Distribution window opens.

For information on selecting protocols for which you want to gather statistics, refer to "Using the Protocol Directory" on page 66.

*** Note:** Changes made to the Protocol Directory will be reflected in the Protocol Distribution bar graph after the device is polled.

For information on generating reports, refer to "Generating Reports" on page 16.

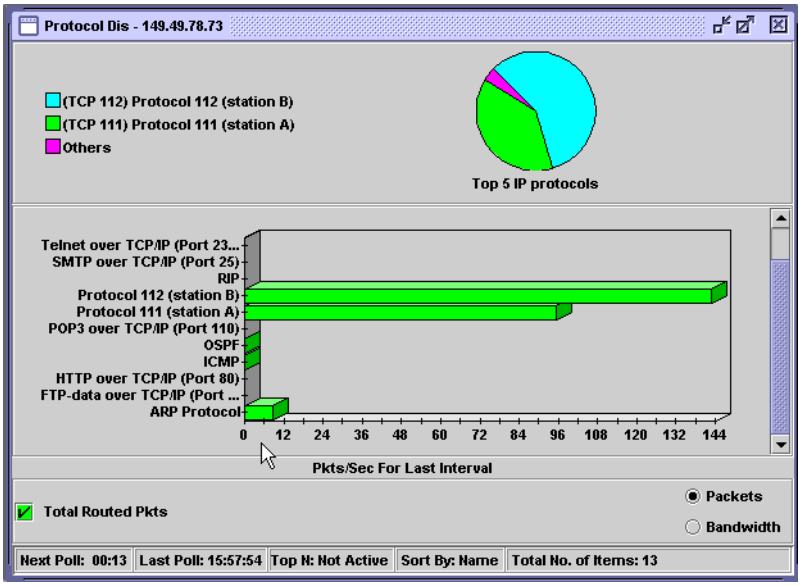
Selecting Protocols to Display

By default, information from all protocols listed in the Default Protocols and User Protocols windows of the Protocol Directory dialog box are displayed in the Protocol Distribution window. You can limit the information being displayed to the most active protocols using TopN filters. For more information, refer to "Using the Define TopN Filter Dialog Box" on page 86.

Protocol Distribution Window

The following graphic provides an example of the Protocol Distribution window.

Figure 9-1. Protocol Distribution Window



The Protocol Distribution window is organized as follows:

- The title of the Protocol Distribution window shows the IP address of the switch.
- The upper part of the window includes a pie chart displaying the relative amounts of the top 5 IP protocols compared to the other protocols.

  The pie chart is updated each time the device is polled. It is also updated when the display mode is changed in the Option dialog box (refer to "Using the Options Dialog Box" on page 74).

- The bottom portion of the Protocol Distribution window contains a bar graph representing the following:
  - The Y axis represents the protocols selected to monitor in the Protocol Directory dialog box (refer to "Using the Protocol Directory" on page 66).
  - The X axis represents the rate of IP traffic through the device in packets per second. Each bar represents the number of packets per second for a specific protocol.
- Checkboxes enable displaying packets or bandwidth in the bar graph.

*** Note:** If the device stops responding, Protocol Distribution will display the last data received until communication is restored.

Using the Protocol Directory

Using the Protocol Directory dialog box, you can view and configure the protocols and specific TCP/UDP ports that an Avaya C460 router module is monitoring. Based on the protocols and TCP/UDP ports selected in Protocol Directory, you can use the Protocol Distribution tool to monitor network traffic organized by protocol and TCP/UDP port number.

This section contains the following topics:

- **Default and User Defined Protocols** - An overview of constant and user defined protocols.
- **TCP/UDP Port Numbers** - An overview of how TCP/UDP port numbers are used in Protocol Directory.
- **Using Protocol Directory** - Instructions on using the Protocol Directory dialog box.

Default and User Defined Protocols

Protocol Directory automatically includes a number of popular protocols for the Avaya C460 router modules to monitor, referred to as Default Protocols, listed in the table below. In addition, you can include other protocols for monitoring by specifying corresponding TCP/UDP ports, referred to as User Defined Protocols.

Default Protocols include a number of network and transport protocols (Layers 3 and 4 in the OSI seven-layer model), such as IP and ARP, as well as many popular application protocols (Layer 7), such as Telnet and SMTP.

User Defined Protocols are TCP/UDP port numbers corresponding to application protocols (Layer 7) you select for the Avaya C460 router module to monitor.

The following table provides a list of the Default Protocols with a description of the protocols.

Table 9-1. Default Protocols

Protocol	Description
IP	Total IP packets travelling through the device.
ARP	ARP packets travelling through the device.
VRRP	VRRP packets travelling through the device.
ICMP	ICMP packets travelling through the device.
OSPF	OSPF packets travelling through the device over IPX.
RIP	RIP packets travelling through the device.

The following table provides a list of the seven initial User Protocols with a description of the protocols.

Table 9-2. User Protocols

Protocol	Description
FTP over TCP/IP	FTP packets travelling through the device over IP.
Telnet over TCP/IP	Telnet packets travelling through the device.
SMTP over TCP/IP	SMTP packets travelling through the device.
HTTP over TCP/IP	HTTP packets travelling through the device.
POP3 over TCP/IP	POP3 packets travelling through the device.

Table 9-2. User Protocols (Continued)

Protocol	Description
SNMP over UDP/IP	SNMP packets travelling through the device.
SNMPtrap over UDP/IP	SNMP trap packets travelling through the device.

TCP/UDP Port Numbers

TCP/UDP port numbers are included in packets sent over a network using either the TCP or the UDP transport layer protocol. The TCP/UDP port number indicates how to apply an application layer protocol to the data at the receiving end. For example, port 25 is associated with the SMTP application protocol, and port 23 is associated with the Telnet application protocol. A single application may use several different TCP/UDP port numbers for various kinds of communication functions it performs.

There are three ranges of TCP/UDP port numbers:

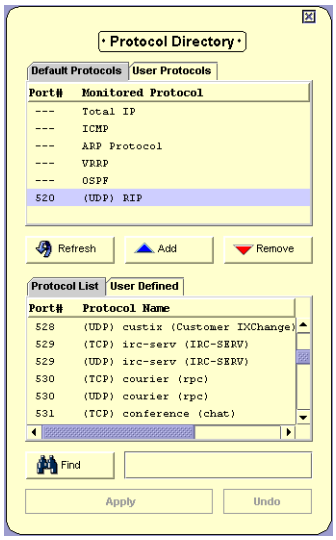
- **TCP/UDP ports 0 - 1023** - Well Known Port Numbers. Well Known Port Numbers represent basic network services that are widely available using standard TCP/UDP port numbers. Well Known Port Numbers are assigned by the IANA (Internet Assigned Numbers Authority). On many platforms, the ways in which these TCP/UDP ports can be used are restricted by the system.
- **TCP/UDP ports 1024 - 49151** - Registered Port Numbers. Registered Port Numbers represent specific network services that have been registered by the IANA at the request of a vendor or organization.
- **TCP/UDP ports 49152 - 65535** - Private Port Numbers. Private Port Numbers are available for unrestricted use by applications. The same Private Port Number might be used for different purposes by different applications.

Using Protocol Directory

To configure the protocols to monitor:

1. Click  . The Protocol Directory dialog box opens.

Figure 9-2. Protocol Directory Dialog Box



The Protocol Directory dialog box is organized as follows:

- The upper section of the Protocol Directory dialog box displays a list of Default Protocols on one tab and a list of User Protocols on the other tab, both which are read from the device. These are the protocols that the device monitors. There are six permanent Default Protocols, and initially seven User Protocols that you can replace with protocols from the tabs below.
- The lower section of the Protocol Directory dialog box displays a Protocol List of known protocols. This list is used to select the protocols that you want to monitor. In addition, you can add a new protocol to the list, using the User Defined tab.

Update the User Protocols list and click **Apply** to update the device. The changes in the Protocol Directory will be reflected in Protocol Distribution after the next time the device is polled.

This section discusses the following topics:

- **Adding Protocols**
- **Adding a User Defined Protocol**
- **Deleting Protocols**

- **Refreshing the Protocol List**
- **Searching for a Protocol**

Adding Protocols

The User Protocols list can only contain seven protocols. Before adding a protocol when there are already seven, you must remove a protocol from the list. For more information on deleting protocols, refer to "Deleting Protocols" on page 71.

To add listed protocols to the User Protocols list:

Double-click the protocol to monitor in the Protocol List.

Or

Select one or more protocols in the Protocol List, and click **Add**. The selected protocol is added to the User Protocols list and is highlighted in cyan.

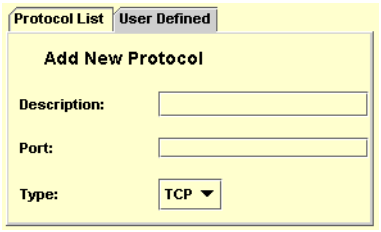
Adding a User Defined Protocol

This feature enables you to add a new protocol that does not exist in the Protocol List or Active Protocols List.

To add a new protocol:

1. Select the **User Defined** tab.

Figure 9-3. User Defined Protocol Dialog Box



2. Enter the protocol description in the Description field.
3. Enter the port number in the Port field, an integer from 1 to 8191.
4. Select the port type, UDP or TCP, from the Type pull-down list box.
5. Click **Add**. The new protocol is added to the User Protocols list highlighted in cyan.
6. Click **Apply**. The new protocol information is sent to the device.

Deleting Protocols

To delete protocols from the list of protocols to monitor:

1. Double-click the protocol to delete in the User Protocols List.

   Or

   Select one or more protocols to delete in the User Protocols List and click **Remove**. The removed protocol is highlighted in red.

2. Click **Apply**. The protocol is removed from the device's list of protocols.

Refreshing the Protocol List

To refresh the list of Active Protocols from the device, click **Refresh**. The device is polled, and all currently active protocols are listed in the Active Protocols list, and the User Protocols list is refreshed.

Searching for a Protocol

To search for a specific protocol in the Active List or Protocol List:

1. Click in the list you want to search to make it active.
2. Enter a number to search for the Port Number.

   Or

   Enter a letter to search for the Protocol Name.

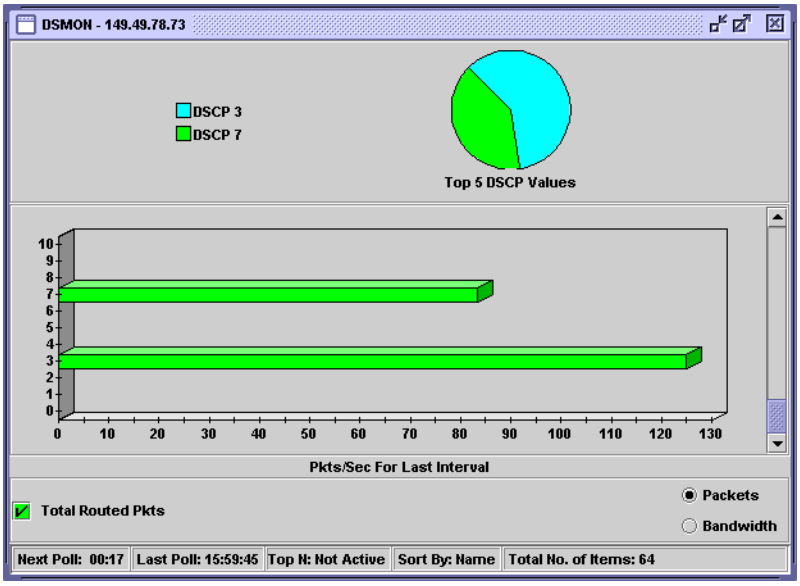
3. Click **Find**.

*** Note:** In each of the lists, you can type the first number of the port number or the first letter of the Protocol Name to go to the next instance in the list.

Viewing DSCP Statistics

The following graphic provides an example of the DSCP Statistics window for viewing DSCP statistics.

Figure 9-4. DSCP Statistics Window



The DSCP Statistics window is organized as follows:

- The title of the DSCP Statistics window shows the IP address of the switch.
- The upper part of the window displays a pie chart with the relative distribution of the traffic of the top 5 non-zero DSCP protocols compared to all other non-zero DSCP protocols.

  The pie chart is updated each time the device is polled. It is also updated when the display mode is changed in the Option dialog box (refer to "Using the Options Dialog Box" on page 74).

- The bottom portion of the DSCP Statistics window contains a bar graph representing the following:
  - The Y axis represents the DSCP protocols.
  - The X axis represents the rate of IP traffic through the device in packets per second.Each bar represents traffic with DSCP headers.
- Checkboxes enable displaying packets or bandwidth in the bar graph.

*** Note:** If the device stops responding, DSCP displays the last data received until communication is restored.

A Using Avaya C460 SMON Dialog Boxes

This appendix consists of dialog boxes that appear within Avaya C460 SMON.

*** Note:** In Device SMON, some of the dialog boxes can only be opened by selecting the relevant menu item.

The following topics are discussed:

Using the Options Dialog Box

This dialog box enables you to change the options for Device SMON for the Avaya C460 Device.

To access the Options dialog box:

Click  .

Or

Select **File > Options**. The Options dialog box opens.

The Options dialog box contains the following tabs, depending on the module selected:

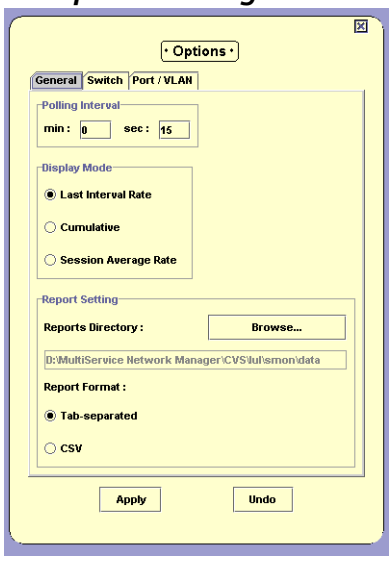
- General Tab
- Switch Tab
- Port/VLAN Tab
- Proto Dist/DSMON Tab

General Tab

This dialog box enables you to change the options for Device SMON for the Avaya C460 Device.

To open the General tab, click the **General** tab at the top of the Options dialog box. The General tab opens.

Figure A-1. Options Dialog Box - General Tab



The General Options dialog box enables you to change the following options:

- Polling Interval
- Display Mode
- Report Setting

Polling Interval

The Polling Interval option allows you to configure the way in which information is collected. If you make the polling interval smaller, you receive more accurate data at the expense of using more network resources. The objective is to use the ideal polling interval that provides accurate data using minimum network resources.

To change the polling interval, enter the number of minutes and seconds for the new polling interval in the min and sec fields.

*** Note:** The polling interval must be between 15 seconds and 59 minutes and 59 seconds.

*** Note:** The new polling interval takes effect when the device is next polled.

Display Mode

The Display Mode option allows you to select one of three display modes. Select a display mode using the radio buttons.

The display mode options are:

- Last Interval Rate - The statistics gathered since the last poll.
- Cumulative - The accumulated statistics gathered since the start of the session.
- Session Average Rate - The average of the statistics per polling interval since the start of the session.

Report Setting

The Report Setting option enables you to select a default directory for saving reports and configure the report format.

To select a default directory for saving reports:

1. Click **Browse**. A directory browser window opens.
2. Navigate to the directory in which you want to save reports.
3. Click **Open**. The path appears in the Reports Directory field.

Select a report format using the radio buttons.

The report format options are:

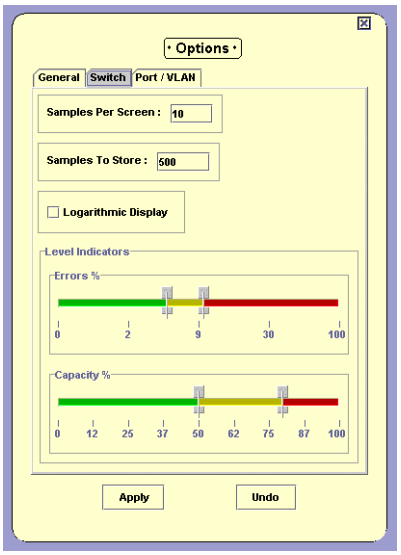
- Tab-separated - The report is formatted as a tab-delimited file.
- CSV - The report is formatted as a comma-delimited file.

Switch Tab

This tab enables you to change the display options for Switch Statistics for the Avaya C460 Device.

To access the Switch tab, click the **Switch** tab at the top of the Options dialog box. The Switch tab opens.

Figure A-2. Options Dialog Box - Switch Tab



*** Note:** Changes made in the Switch Statistics Options dialog box apply to Switch Statistics and Extended Port Statistics.

The Switch Options dialog box enables you to change the following options:

- **Samples Per Screen**
- **Samples To Store**
- **Logarithmic Display**
- **Level Indicators**

Samples Per Screen

The Samples Per Screen option enables you to configure the number of samples visible in the Traffic Graph. To change the number of samples visible on the screen, enter a number in the Samples Per Screen field.

*** Note:** The number of samples per screen must be between 3 and 500.

Samples To Store

The Samples To Store option enables you to configure the number of samples saved in the Traffic Graph. You can scroll the Traffic Graph to view all of the saved samples. To change the number of stored samples, enter a number in the Samples To Store field.

*** Note:** The number of samples to store must be between 100 and 8000.

Logarithmic Display

The Logarithmic Display option enables you to specify whether or not you want the Traffic Graph to be displayed on a logarithmic scale. This is useful when the values in the graph are small.

To view the traffic graph with a logarithmic display, check the Logarithmic Display checkbox.

To view the traffic graph with a non-logarithmic display, uncheck the Logarithmic Display checkbox.

Level Indicators

The Level Indicators option enables you to change the appearance of the gauges at the top of the Switch Statistics window. This allows you to determine the range corresponding to the colors of the gauge.

To configure the level indicators, slide the markers for each of the gauges to the desired percentages.

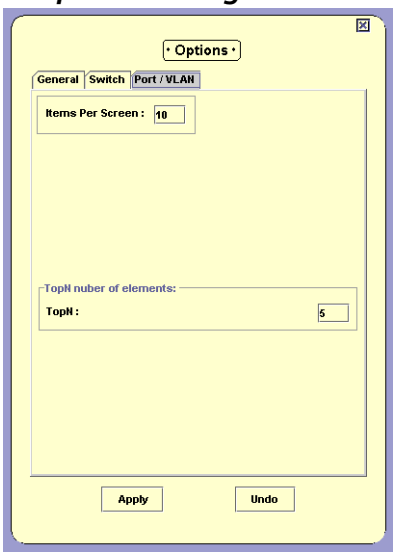
The leftmost marker sets the percentage at which the color on the gauge changes from green to yellow. The rightmost marker sets the percentage at which the color on the gauge changes from yellow to red.

Port/VLAN Tab

This tab enables you to change the display and TopN filtering options for Port and VLAN Statistics for the Avaya C460 Device.

To access the Port/VLAN tab, Click the **Port/VLAN** tab at the top of the Options dialog box. The Port/VLAN tab opens.

Figure A-3. Options Dialog Box - Port/VLAN Tab



The Port/VLAN Options dialog box enables you to configure the number of ports, LAGs, and VLANs visible in the Port and VLAN Statistics windows and the number of ports, LAGs, and VLANs displayed when TopN filtering is active.

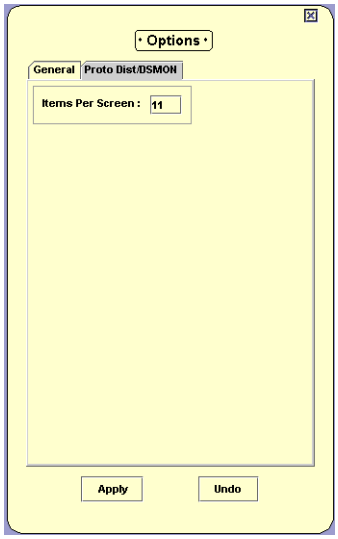
- To change the number of items visible on the screen, enter a number in the Items Per Screen field. The number of items per screen must be between 1 and 15.
- To change the number of items displayed when TopN filtering is active, enter a number in the TopN field. The number of items must be between 1 and 15.

Proto Dist/DSMON Tab

This tab enables you to change the display options for Protocol Distribution and DSCP Statistics for the Avaya C460 Device.

To access the Proto Dist/DSMON tab, Click the **Proto Dist/DSMON** tab at the top of the Options dialog box. The Proto Dist/DSMON tab opens.

Figure A-4. Options Dialog Box - Proto Dist/DSMON Tab



The Proto Dist/DSMON tab enables you to configure the number of items visible in the Protocol Distribution and DSMON windows.

- To change the number of items visible on the screen, enter a number in the Items Per Screen field. The number of items per screen must be between 1 and 15.

Using the Report Now Dialog Box

This dialog box enables you to generate a report with the statistics from the last time the device was polled.

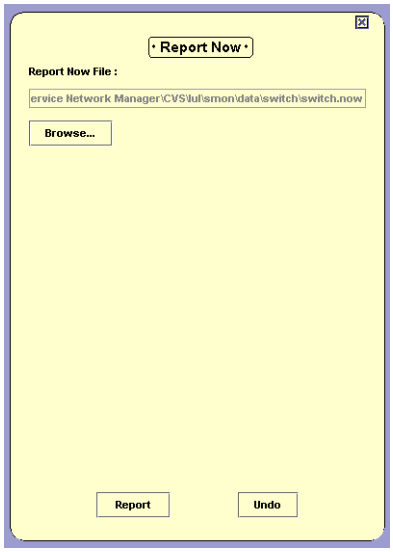
To access the Report Now dialog box:

1. Click  .

   Or

   Select **File > Report Now**. The Report Now dialog box opens.

Figure A-5. Report Now Dialog Box



2. To change the filename and directory in which to save the report:

   a. Click **Browse**. A file browser window opens.

   b. Select a directory and filename for the reports.

   c. Click **Open**.

3. Click **Report**. The report is generated.

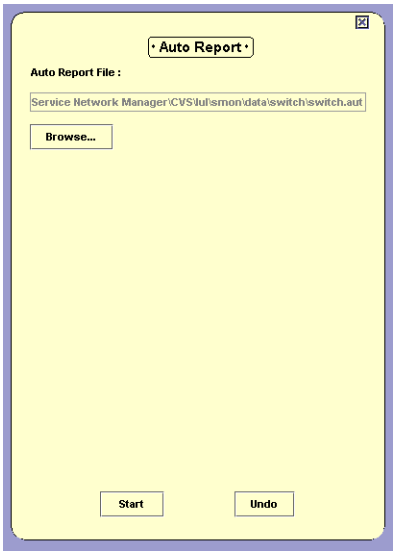
Using the Auto Report Dialog Box

This dialog box enables you to start and stop generating reports automatically.

To access the Auto Report dialog box:

1. Select **File > Auto Report**. The Auto Report dialog box opens.

Figure A-6. Auto Report Dialog Box



2. To change the filename and directory in which to save the reports:
   a. Click **Browse**. A file browser window opens.
   b. Select a directory and filename for the reports.
   c. Click **Open**.
3. Click **Start**. The first report is generated immediately. Subsequent reports are generated according to the polling interval.

CAUTION

Auto Reports are automatically saved to the network management station (NMS). If Auto Reports are generated on many devices for a long period of time, and none of the files are deleted, the NMS's hard disk may become full.

If this occurs, stop the applications that are generating automatic reports and delete the files that are not required.

To stop generating Auto Reports:

1. Select **File > Auto Report**. The Auto Report dialog box opens.
2. Click **Stop**.

Or

1. Close the application for which you are running the Auto Report. Auto Reports are no longer generated.

Using the Find Dialog Box

Depending on the application from which you have initiated this option, the Find option allows you to locate a specific VLAN/port/LAG intersection in the application window.

To search:

1. Click  .

   Or

   Select **Edit > Find**. The Find dialog box opens.

   The information you are prompted for in the Find dialog box differs depending on the application from which you have initiated it.

   For more detail, refer to “Finding a Port or LAG” on page 84 or “Finding a VLAN” on page 85.

2. Enter the information in the dialog box and click **Find**. The VLAN/port/LAG intersection found is highlighted in the application for easy identification.

To remove the highlight from the application window, click the graph. The highlight disappears.

*** Note:** The Find button changes to Find Next until all instances of the search information have been found.

*** Note:** Since the number of VLANs/ports/LAGs may change between sampling intervals, the one you search for may move out of focus with the next refresh. In this case, you may search again or scroll the display.

Finding a Port or LAG

There are several ways to enter a value to find a port or LAG.

To search for a port or LAG by name:

1. Click the Port/LAG Name option button.
2. Enter the port or LAG name or part of the port or name in the Port/LAG Name field.
3. Click **Find**.

*** Note:** If you enter only part of the name, SMON will find the first time the value appears.

To search for a port or LAG by number:

1. Click the Port/LAG Name option button.
2. Enter the port or LAG number in the Port/LAG Number field.
3. Click **Find**.

Finding a VLAN

There are several ways to enter a value to find a VLAN.

To search for a VLAN by name:

1. Click the VLAN Name option button.
2. Enter the VLAN name or part of the port or name in the VLAN Name field.
3. Click **Find**.

*** Note:** If you enter only part of the name, SMON will find the first time the value appears.

To search for a VLAN by number:

1. Click the VLAN Name option button.
2. Enter the VLAN number in the VLAN Number field.
3. Click **Find**.

Using the Define TopN Filter Dialog Box

You can also filter using the TopN option. TopN filtering differs from item filtering in that SMON chooses the items with the heaviest traffic. The TopN filter produces a report for the 1-15 (*N*) most active items on the network.

SMON chooses the TopN items by a rate base which you select from the Define TopN Filter dialog box. SMON measures the rate base for all the items to find the TopN items and then displays these items and their statistics.

*** Note:** If you previously defined a filter, TopN will select the TopN items from the specified subset.

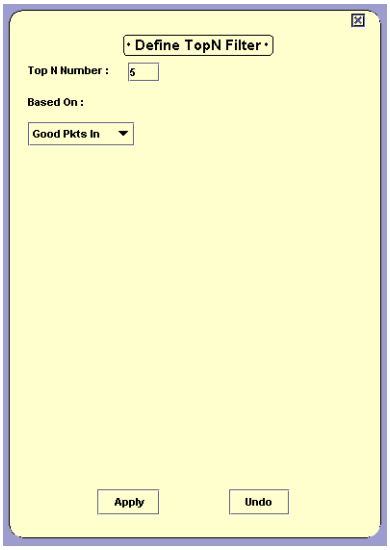
To select the criterion for TopN Configuration:

1. Click  .

   Or

   Select **Actions > Define Top N Filter**. The Define TopN Filter dialog box opens.

Figure A-7. Define TopN Filter Dialog Box



2. Select the number of items and the criterion for the TopN filter.

*** Note:** Filtering changes are only applied after clicking **Apply**.

The dialog box contains the following fields:

- TopN Number - Enter the number of items to be displayed when you activate TopN.
- Based On - Select the criterion for deciding which items fall in the TopN. The rate base can be any one of the available counters.

Using the Find Top5 Peaks Dialog Box

In Switch Statistics and Extended Port Statistics, you can use the Find Top5 Peaks option to find the largest value of any counter. This can help you find when a problem occurred or when a problem was most severe.

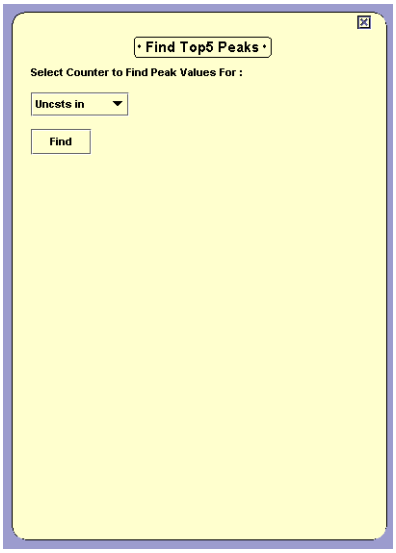
To select the criterion for Find Top5 Peaks:

1. Click  .

   Or

   Select **Edit > Find**. The Find Top5 Peaks dialog box opens.

Figure A-8. Find Top5 Peaks Dialog Box



2. Select a counter in Switch Statistics or Extended Port Statistics.
3. Click **Find**. The display scrolls the graph to the peak value and a vertical line appears at the peak value. The pie values at the top are correct for this time period. The graph is frozen.

To find the next highest peak, click **Find Next**. The displays scrolls to the next highest peak value in the graph.

In Switch Statistics and Extended Port Statistics, all counters are listed in the Find Top5 Peaks dialog box, including those counters not currently displayed in the Traffic Graph.

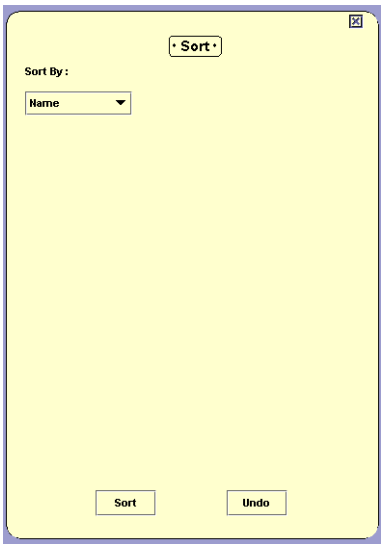
Using the Sort Dialog Box

You may sort the display by one of the available categories in the list.

To perform a sort:

1. Select **Actions > Sort**. The Sort dialog box opens.

Figure A-9. Sort Dialog Box



2. Select the appropriate sorting criterion from the Sort By drop-down listbox.
3. Click **Sort**. Sorting begins immediately. New information is sorted at each subsequent polling.

When sorting by Name, the bars appear in ascending order from bottom to top. When sorting by packets, the bars appear in descending order (most traffic at the bottom, least traffic at the top).

B Setting Up the SMON License

The Avaya MultiService Network Manager with SMON Manager package contains a license that allows you to use SMON on a permanent basis. The Avaya MultiService Network Manager package does not include this license. Instead, a trial version of SMON is included. This trial version expires 60 days after its first use. In addition, an embedded license is required for SMON for Avaya C460 Devices.

For information on entering the SMON license, refer to the *Avaya MultiService SMON Manager User Guide*.

To use SMON with Avaya C460 Devices, you must enter a valid embedded license via the Avaya C460 CLI. A unique License is required for each Avaya C460 Device regardless of the number of modules in the device. A group License is valid for the number of devices for which it was purchased.

For information on entering the Avaya C460 embedded SMON License, refer to the *SMON for Avaya C460 Installation Guide*.

Device SMON for Avaya C460 Devices does not require a license for the first 60 days. After 60 days, this application will not run unless you enter a valid embedded SMON license.

Index